



*ANYSEC* 安全网关  
使用说明书

版权所有：深圳市中科网威科技有限公司

## 声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。  
其版权归深圳市中科网威科技有限公司所有。  
未经本公司书面许可，本手册的任何部分不得以任何形式手段复制或传播。

## NOTICES

Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

**© Copyright 2009 -2012 by Anysec-Tech. Co., Ltd. All Right Reserved.**

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without express written permission of Anysec Co., Ltd.

ANYSEC 是深圳市中科网威科技有限公司注册商标。所有其他商标均属于有关公司所有。

## 目录

第一章	介绍	6
➤ 目的		6
➤ 版本		6
➤ 适用对象		6
第二章	产品说明	7
➤ 产品概述		7
◇ 面板视图（设备不同，视图略有不同）		7
➤ 应用拓扑		8
第三章	产品安装	9
➤ 连接		9
➤ 登陆		9
第四章	基于 Web 的管理器	10
➤ 工具栏功能		11
➤ 主菜单功能		11
第五章	基于 CLI 的管理器	12
第六章	快速安装向导	14
第七章	WEB 配置管理	20
➤ 系统管理		20
◇ 状态		20
◇ 设置		23
◇ 管理员		26
◇ 证书		28
◇ 维护		30
➤ 网络管理		32
◇ 安全区		32
◇ 接口		32
◇ 路由		35

◇ DNS .....	37
◇ DHCP .....	38
◇ 会话 .....	41
◇ 链路 .....	44
☉ 用户管理 .....	45
◇ 用户 .....	45
◇ 用户组 .....	46
◇ RADIUS .....	47
◇ LDAP (略) .....	48
◇ POP3 (略) .....	48
◇ TACACS+ (略) .....	48
☉ 防火墙 .....	48
◇ 策略 .....	48
◇ 地址 .....	50
◇ 服务 .....	53
◇ 时间 .....	55
◇ 地址转换 .....	56
◇ IP/MAC 绑定 .....	57
☉ VPN 管理 .....	59
◇ 点点通 .....	59
◇ 设备隧道管理 .....	59
◇ PPTP .....	66
◇ IPSEC .....	67
◇ SSL VPN .....	72
◇ 移动客户端 .....	74
◇ 配置客户端 .....	76
☉ 行为管理 .....	80
◇ 定义行为管理策略 .....	80
◇ DNS 定义 .....	82
◇ 网页定义 .....	85
◇ 文件定义 .....	88
◇ 邮件审计 .....	89

◇ 带宽控制 .....	92
⊖ 网络监控 .....	92
◇ 定义监控规则 .....	92
◇ 监控选项 .....	93
◇ 流量监控（具体功能依产品型号不同而不同） .....	94
◇ DNS 监控 .....	96
◇ 网页监控 .....	97
◇ 邮件监控 .....	98
◇ 聊天监控 .....	98
◇ P2P 监控 .....	99
◇ 娱乐监控 .....	100
◇ FTP 监控 .....	101
⊖ 日志审计 .....	101
◇ 系统日志 .....	102
◇ 防火墙日志 .....	102
◇ VPN 日志 .....	102
◇ 日志配置 .....	104
第八章 Console 配置 .....	105
⊖ 连接 .....	105
⊖ 配置电脑 .....	105
⊖ 基本配置 .....	107
第九章 .....	常见问题解答 109
⊖ 故障处理流程 .....	110
附：点点通配置实例 .....	112
⊖ 客户背景介绍 .....	112
⊖ 总部点点通管理平台配置 .....	112
⊖ 分支节点配置： .....	118

## 第一章 介绍

欢迎使用 ANYSEC 网络安全产品，构筑企业安全上网环境。

ANYSEC 全系列产品提供多种可靠的网络安全技术增强企业网络的安全性，避免了网络资源的误用和滥用，帮助企业更有效的使用通讯资源的同时不会降低网络的性能。

### ☞ 目的：

本手册提供 ANYSEC 安全网关系列产品的硬件使用安装和调试配置操作说明，并随购买的产品一并附给用户。

### ☞ 版本：

适用设备型号：ANYSEC S 系列、M 系列以及 T 系列。（某些功能、显示略有不同）

### ☞ 适用对象：

本手册适用于购买我公司 ANYSEC 安全网关系列产品的用户。要求使用者必须具备一定的网络知识和 TCP/IP 基础知识，并且熟悉电子设备的使用和保护。

## 第二章 产品说明

### ○ 产品概述

ANYSEC 安全网关系列产品是基于 Anysec OS (Linux) 开发的安全智能网关产品，具备网络行为管理、流量监控、邮件审计、防火墙、VPN、代理上网、上网认证等多种功能。为用户提供全方位网络安全互联解决方案。

目前ANYSEC 安全网关系列产品已经通过公安部计算机信息系列安全产品质量监督检验中心检验，并且获得了防火墙和 VPN 安全专用产品销售许可证书。

#### ◇ 面板视图（设备不同，视图略有不同）



图 2-1： 设备面板视图

LAN 指示灯：局域网连接 LAN 状态指示  
广域网连接 WAN 状态指示

WAN 指示灯：

System 指示灯：系统状态指示  
电源状态指示

Power 指示灯：

WAN：广域网接口  
接口

LAN：局域网

Console 口：串口线配置接口  
定义接口

E 口：支持自

## 应用拓扑

以深圳、北京、香港为例组建常见应用的 IP VPN 网络，使用 ANYSEC 安全网关的网络应用拓扑如下示：

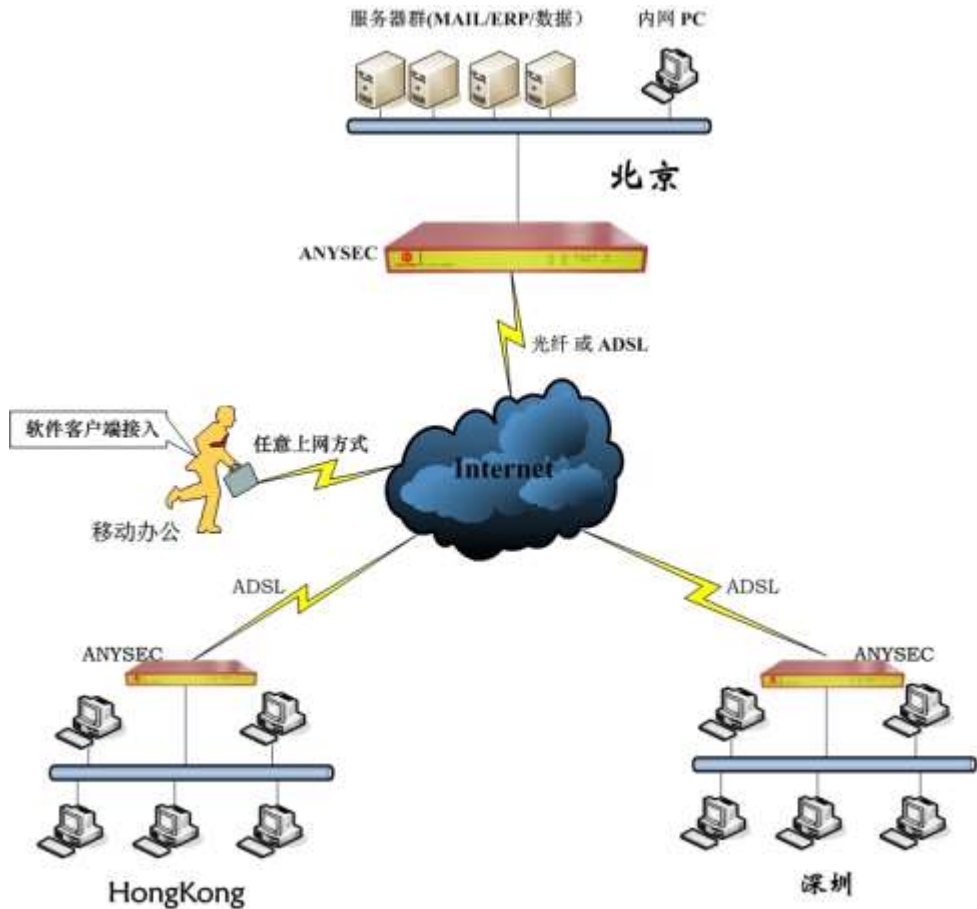


图 2-1：设备应用拓扑图



## 第三章 产品安装

### ☞ 连接

首次连接并准备配置 ANYSEC 设备时，请参照一下图示连接：

#### 1. 单机环境下设备接线参考图：

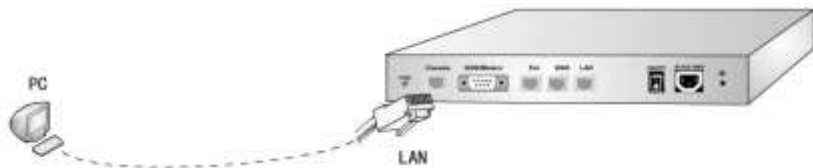


图 3-1：与单机连线图

#### 2. 交换机环境下设备接线参考图

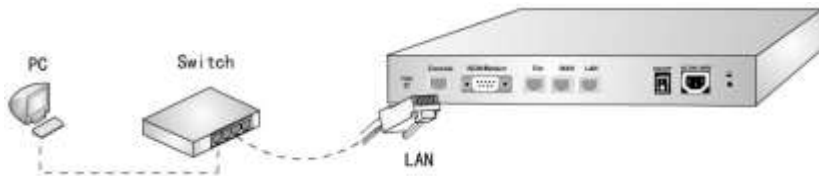


图 3-1：与交换机连线图

### ☞ 登陆

ANYSEC 安全网关系列设备缺省配置说明：

- ◇ LAN/E0 口缺省 IP： 192.168.0.99                      缺省端口：8080
- ◇ 缺省登陆账号： 用户名：admin                      密码：anysec
- ◇ 将配置电脑和 ANYSEC 设备缺省 LAN IP 为同一个网段，例如：  
192.168.0.88
- ◇ 在 IE 浏览器中访问：<http://192.168.0.99:8080> 即可进入登陆界面

## 第四章 基于 Web 的管理器

本章介绍有关 Anysec 设备基于 Web 管理器管理接口的功能。

通过运行 Internet 浏览器的任何计算机使用 HTTP 或一个安全的 HTTPS 连接, 您便能够配置并管理 Anysec 设备。

默认的 HTTP 端口是 8080, 默认的 HTTPS 端口是 8443。

Anysec 设备基于 Web 的管理器界面图:



图 4-1: Anysec 设备 Web 管理界面

使用基于 Web 的管理器可以配置大部分的 Anysec 设置以及监控 Anysec 设备的状态。使用基于 Web 管理器进行的配置更改无需重新设置防火墙或中断服务便可以生效。配置完成后, 可以保存设置作为备用。所保存的配置在任何时间都可以恢复。

## ② 工具栏功能

基于 Web 管理器中右上角的工具栏可以访问 Anysec 设备几项重要的功能。

 向导	快速安装向导功能
 保存	配置保存功能
 帮助	帮助功能
 退出	退出功能

## ② 主菜单功能

基于 Web 管理器左边类似 Outlook 菜单风格的主菜单提供了 Anysec 设备的各种配置功能。

<b>系统管理</b>	提供了系统状态查看、系统设置、管理员操作、证书管理、系统维护等子功能。
<b>网络管理</b>	提供了安全区定义、网络接口管理、路由管理、DNS/DDNS、DHCP 服务、会话管理和链路管理功能。
<b>用户管理</b>	提供了用户和用户组的管理，支持多种认证方式。
<b>防火墙</b>	提供配置防火墙访问控制策略。
<b>VPN 管理</b>	提供多种 VPN 服务。
<b>行为管理</b>	提供上网行为管理策略服务。
<b>网络监控</b>	提供上网监控服务。
<b>日志审计</b>	提供详细的设备日志功能。

(注：系统功能依设备型号不同而有所不同)

## 第五章 基于 CLI 的管理器

本章介绍有关 Anysec 设备基于 CLI 管理器管理接口的功能。

通过运行 TELNET 或 SSH 的任何计算机使用 TELNET 或一个安全的 SSH 连接，您便能够配置并管理 Anysec 设备。

默认的 TELNET 端口是 8023，默认的 SSH 端口是 8022。

Anysec 设备基于 CLI 的管理器界面如下图：

```
*****
*           Welcome to Anysec UFM System           *
*                                                                 *
* Anysec-Network <ShenZhen> Co., Ltd Copyright *
*****

Welcome admin it is Wed Nov 11 15:52:13 CST 2009
admin@> #
^
behavior      Enter Behavior Module
cls           Clear the screen
diagnose      Enter the Diagnose Module
execute       Enter Execute Module
exit          Exit this CLI session
firewall      Enter Firewall Module
help          Display an overview of the CLI syntax
history       Display the current session's command line history
log           Enter Log Module
logout        Logout of the current CLI session
netmonitor    Enter Netmonitor Module
network       Enter Network Module
showall       Show current running configuration
system       Enter System Module
user          Enter User Module
vpn           Enter UPN Module

admin@> #
```

图 5-1：基于 CLI 的管理器界面图

基于 CLI 的管理器提供了专业级的设置管理平台，在安全性要求较高的应用中，可以通过设备串口登陆，通过 CLI 管理器来配置设备，避免了网络配置过程中的不



安全因素。

## 第六章 快速安装向导

本章是关于如何使用快速安装向导来配置 Anysec 设备的内容描述。

### 1、点击工具栏的快速安装向导按钮



图 6-1:快速安装向导界面

快速安装向导的目的是协助您通过最简单的方式将 Anysec 设备接入 Internet。  
注意：如果您以前已对该设备进行了部分配置操作，然后又通过快速安装向导来重新配置设备的话，您之前配置的所有信息将会无效。

### 2、设置许可证



图 6-2:许可证设置界面

Anysec 设备的许可证分为两种：测试许可证和正式授权许可证。  
测试客户选择申请试用，试用时间一般为一到二周，当设备检测到试用时间已结

束时，将会在 web 界面上提示您许可证已过期。这时您需要联系您的设备提供商以获取正式授权许可证。

正式客户先选择下载授权许可证申请，申请文件的后缀是 dlr，将该文件提交给您的设备提供商，以获取正式授权许可证文件，然后点击导入授权许可证导入正式许可证文件。

**注意：**如果您的设备提供商已经将正式授权许可证导入了设备时，您可以选择“跳过”按钮，忽略该功能配置。

### 3、设置设备运转模式



图 6-3: 设备运行模式设置界面

Anysec 设备通过快速安装向导能够支持路由/NAT 模式和透明模式两种接入方式，用户可以根据自身网络拓扑选择设备的运转模式。

路由/NAT 模式：打开设备路由功能，作为网关使用。

透明模式：关闭设备路由功能，网桥模式。

### 4、修改管理员密码



图 6-4:管理员密码修改界面

您可以通过该界面修改管理员 admin 的密码，Anysec 设备出厂时默认密码是 anysec。

## 5、设置网络接口

对于不同的设备型号，配置网络接口的数目是不同的。Anysec 设备将会要求您对所有设备接口进行配置。



图 6-5:网络接口配置界面（非广域网）

根据需求配置相关网络接口参数。例如：

选择接口类型为“非广域网”，工作模式为“ROUTE”，IP 地址为“192.168.9.1”，网络掩码为“255.255.255.0”；





图 6-6: 网络接口配置界面（广域网）

根据需求配置相关网络接口参数。例如：

选择接口类型为“广域网”，工作模式为“NAT”，地址模式为“PPPOE”。用户名为当地 ISP 提供商提供的用户名，密码为当地 ISP 提供商提供的密码，DNS 覆盖则为不选择；

NAT：广域网工作模式；

固定 IP：光纤、城域网等固定 IP 广域网接入方式；

PPPOE：ADSL 等拨号接入广域网方式；

DHCP：某些特殊上网环境用户，自动获取运营商 IP 接入方式。

## 6、设置 DNS



图 6-7: DNS 设置界面

配置主 DNS 服务器，根据当地实际 DNS 填写。（请咨询相关工程师或搜索您所在地

DNS 信息)

例如 **深圳电信**：主 DNS 服务器：202.96.134.133；从 DNS 服务器：  
202.103.96.112

## 7、设置 DHCP 服务器



图 6-8:DHCP 服务器设置界面

根据实际需求配置 DHCP 服务器，不需要 DHCP 服务器功能可以直接选择“跳过”。

**DHCP**：自动分配 IP 地址功能。

## 8、设置点点通隧道参数



图 6-9: 点点通隧道设置界面

当您的设备无需用到点点通自动隧道功能时，您可以选择“跳过”按钮忽略该功能配置。

## 8、保存配置



图 6-10: 快速安装配置保存界面

## 第七章 WEB 配置管理

### ○ 系统管理

本章用于描述 Anysec 设备的系统状态查看、设置、访问管理、设备证书管理和设备维护等功能。

#### ◇ 状态

用户点击状态菜单，可以查看设备版本信息、系统资源消耗和设备功能配额。

#### ● 版本信息



图 7-1: 版本信息界面

管理员可以通过版本信息界面查看当前 Anysec 设备的基本情况，例如设备名、设备型号、许可证、软件版本、移动客户端版本、硬件版本、系统架构版本、系统启动时间、系统的运转模式以及当前已运行时间。

**说明：许可证一栏存在如下几种情况：**

- 1、显示“正式授权许可证”，表示该 Anysec 设备里已经导入了正式授权

许可文件。

- 2、显示“试用(过期日:年月日 时间 星期)”，表示 Anysec 设备处于试用状态以及到期的时间。
- 3、显示“没有许可证”，表示当前 Anysec 设备没有许可证，该状态下部分功能不可用。

## ● 系统资源



图 7-2: 信息资源界面

显示系统当前 CPU、内存、虚拟盘及网络会话的情况。

● 功能及配额

系统名称	系统类型	功能及配额	
主模块	功能模块	默认配额	备注
系统管理	CA认证中心	不准备	是否具备CA功能
	密钥设备	具备	是否具备密钥设备
网络管理	PKI设备	具备	支持多少PKI设备(默认软件自带无限制)
	电话机	300000	最大并发电话数
用户管理	EAD认证	具备	是否支持EAD认证功能
	LDAP认证	不准备	是否支持LDAP认证功能
	PIPS认证	不准备	是否支持PIPS认证功能
	TACACS+认证	不准备	是否支持TACACS+认证功能
防火墙	策略	4096	允许设置的防火策略数量
	地址	无限制	是否支持地址列表数量
	端口	无限制	是否支持端口列表数量
	时间	无限制	是否支持时间列表数量
	虚拟IP	无限制	是否支持虚拟IP策略数量
	点选透传中心	具备	是否具备点选透传策略配置及在线下发及设备固件功能
点选透传	点选透传	4096	是否建立点选透传策略数量
	IPSEC	无限制	是否建立IPSEC策略数量
	VPN	无限制	是否建立VPN策略数量

图 7-3: 功能及配额界面

显示当前系统的所具备的功能及性能参数。

## ◇ 设置

用户点击设置菜单，可以对设备进行时间设置、配置双机热备的高可行性功能配置和配置设备运转模式。

### ● 时间设置



图 7-4: 设备时间设置界面

用户可以手工设置 Anysec 设备的系统时间，也可以与 PC 机同步时间，还可以与因特网上的时间同步服务器同步时间。

### ● 双机热备（依产品型号而定，一般低端型号不具备该功能）



图 7-5: 双机热备设置界面

**双机热备功能：**是用于提供设备高可靠性服务的一种功能，通常的做法是提供 2 台或者多台设备模拟成一个虚拟设备，对外提供一个 IP 地址，来提供网络服务。

**工作模式：**分为主模式和运转模式、主模式和备份模式，主模式是处于激活状态下提供正常网络服务的模式，而备份模式则是处于等待激活状态，一旦主模式的设备出现故障，备份设备发现后，就会主动接管网络服务。

**工作接口：**是指双机热备的服务是用于处理哪个网络接口的。

**虚拟 IP 地址：**是双机热备模式下对外提供的统一的 IP 地址。

**热备组号：**是一组优先级，用于指定各个备份设备转换主模式的优先次序。

**抢占状态：**是用于指定是否抢占主模式，主动提供服务的状态。

**服务状态：**是用于指定双机热备服务功能是否激活的状态。

- 运转模式



图 7-6: 设备运行模式设置界面

Anysec 设备提供多种接入方式，可以支持路由/NAT 模式、透明模式和桥接模式及混合模式。用户根据自身网络规划，在运作模式中选择合适的设备接入方



式。注：桥接模式和混合模式只有在中高端产品中才提供。

## ◇ 管理员

用户点击管理员菜单，可以对 Anysec 设备的访问控制进行设置。管理员可以访问 Anysec 设备并配置其操作。在设备初始化安装完成后，默认的配置只有一个用户名为 admin 的管理员账户，其初始默认密码为 anysec。通过连接到基于 Web 的管理器或 CLI，用户也可以配置更多的管理员具有权限的 Anysec 设备的配置的管理访问。

### ● 管理员



图 7-7:新建管理员界面

添加一个新的管理员，可以指定密码、信任的主机和访问管理权限。

### ● 权限



图 7-8:新建权限界面

Anysec 设备的各个功能模块具有权限控制功能，因此用户可以自定义权限

集合，然后赋予指定的管理员，提供设备的多用户多权限管理。

**只读权限：**只能对该模块进行浏览操作，无法进行新建、修改、删除等功能操作。

**读写权限：**能够对该模块进行新建、修改、删除及浏览等所有功能操作

**不可视权限：**无法在界面上看到该模块的任何信息。

## ● 设置



图 7-9:设备管理端口和登录参数设置界面

在设置功能中，用户可以配置 Anysec 设备的各种管理端口和登录参数。

**空闲超时：**当管理员登录界面后多长时间间隔内没有对界面进行任何操作时，Anysec 设备将主动删除本次会话信息并退回到登录界面。默认值为 300 秒。

**认证超时：**当 Anysec 设备具有访问 Internet 的 Web 认证功能时，若用户通过 Web 认证功能认证上网后多长时间间隔内没有对 Internet 进行任何新建连接的访问操作时，Anysec 设备将主动删除该用户的上网许可，并在下次用户访问 Internet 时再次出现认证页面要求进行身份认证。默认值为 1800 秒

**登录失败最大值：**当管理员获非法用户通过 Web 或 CLI 对设备进行管理时，若登录失败次数达到该值，该登录用户的 IP 地址将被加入黑名单以避免重复尝试。

- **黑名单**



图 7-10: 设备登录黑名单列表

当非法用户尝试登陆设备，多次认证失败后，该用户所用的 IP 就会被加入到黑名单中，需要管理员来解除。

- ◇ **证书**

用户点击证书菜单，可以进行符合 X.509 标准的数字证书的相关操作，产生证书请求、管理本机证书、导入其他证书、根证书管理、证书作废列表管理等等。



图 7-11: 证书相关设置界面

- **证书签署请求**

第三方证书签署申请表

- 本机证书
- 远端证书
- CA 证书

中高端设备自带 CA 平台

- 证书作废表

**注意：**该部分使用配置请详见《SecROS UKey 管理员手册》；

如需使用该功能，请联系我司技术工程师协助，技术热线：  
0755-83658229，13510693536（24 小时）

## ◇ 维护

用户点击维护菜单，可以进行设备的配置保存、备份和恢复等操作。

### ● 保存配置

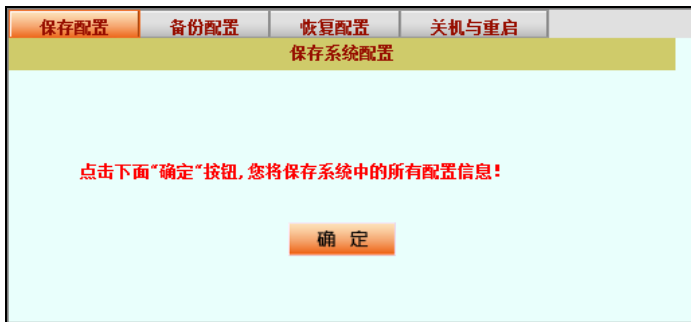


图 7-12: 保存配置界面

保存系统的所有配置信息。

### ● 备份配置

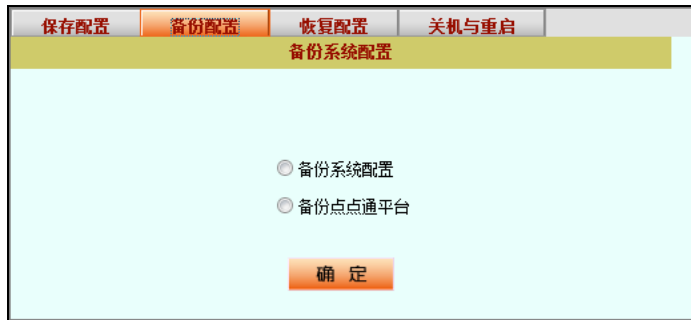


图 7-13: 备份配置界面

备份配置包含两种功能的备份：

- 1、 备份系统配置
- 2、 备份点点通平台（当设备具备点点通平台功能时）

- 恢复配置



图 7-14: 恢复系统配置界面

恢复配置包含三种功能的恢复：

- 1、恢复出厂设置
- 2、恢复系统配置
- 3、恢复点点通平台（当设备具备点点通平台功能时）

- 关机与重启



图 7-15: 设备关机与重启界面

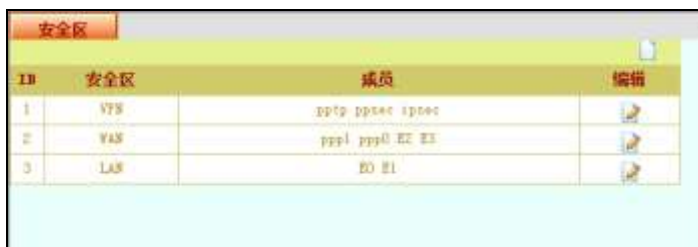
通过系统进行软重启或关机操作。

## 网络管理

本章用于描述如何将 Anysec 设备配置到网络中作为网络安全设备生效。基本的网络设置包括配置 Anysec 设备的接口与用户的网络连接、以及配置 Anysec 的 DNS、DDNS 等设置。

### 安全区

使用安全区可以将相关联的接口划分为一个集合进行管理。安全区名称的定义与防火墙策略有直接关系，所有防火墙策略都是基于安全区来进行配置及管理的。用户可以在安全区列表中添加安全区，编辑及删除安全区。添加安全区时，选择该区域所包含的接口成员。



ID	安全区	成员	编辑
1	VTS	ppp0 ppsoc spnet	[Edit]
2	VAS	ppp1 ppp0 EE EE	[Edit]
3	LAS	E0 E1	[Edit]

图 7-16: 安全区设置界面

### 接口

点击接口菜单，用户可以：

- 1、修改物理接口的属性
- 2、添加并配置 VLAN 子接口（一般低端产品不具备该功能）
- 3、添加接口别名



类型	端口名	IP/Mask	网关	状态	编辑
物理接口	E3(ppp0)	116.214.100.220/255.255.255.255	ping http https telnet ssh snmp	[Status]	[Edit]
物理接口	E2(ppp1)	218.18.209.60/255.255.255.255	ping http https telnet ssh snmp	[Status]	[Edit]
物理接口	E1	192.168.1.1/255.255.255.0	ping http https telnet ssh snmp	[Status]	[Edit]
物理接口	E0	192.168.59.1/255.255.255.0	ping http https telnet ssh snmp	[Status]	[Edit]
隧道接口	gre0	192.168.59.1/255.255.255.255	ping http https telnet ssh snmp	[Status]	[Edit]
隧道接口	cpss0	177.0.0.1/255.0.0.0	ping http https telnet ssh snmp	[Status]	[Edit]
隧道接口	ppp	192.168.100.1/255.255.255.255	ping http https telnet ssh snmp	[Status]	[Edit]
桥接接口	bridge0	0.0.0.0/0.0.0.0		[Status]	[Edit]



图 7-17:接口状态界面

接口类型分为物理接口、隧道接口和桥接接口等多种。  
点击修改按钮，可以修改接口的各种参数。如下图示：



图 7-18:接口设置界面

**接口类型：**分为广域网接口和非广域网接口两种。当该接口所连网线与 Internet 直接连接时，一般选择“广域网”；当该接口所连网线与您做在的内网直接连接时，一般选择“非广域网”。

**工作模式：**分为 ROUTE 模式和 NAT 模式。一般情况下，广域网接口选择“NAT 模式”，非广域网接口选择“ROUTE”模式。

**地址模式：**ISP 提供的 Internet 接入模式，依您的实际情况进行选择。

**ISP 类型：**目前提供有五种选择：电信、网通、铁通、联通或其他。这依您的实际情况进行选择。

**DNS 覆盖：**ISP 提供的 DNS 是否覆盖当前系统中的 DNS 配置信息。


**线路检测 IP：**当您的设备存在多 WAN 链路时，您可以通过设置该检测 IP 以让设备进行自动检测链路是否正常。当设备检查到链路不通时将主动进行链路切

换。注：该检测机制是通过 Ping 的方式进行的，请在填入检测 IP 时确认该 IP 地址是否允许 Ping。

**动态域名：**当该接口与 Internet 连接后是否提供 DDNS 功能。若需要提供动态域名服务的功能，请先在 DDNS 中进行配置，然后在这里进行引用及可。

**安全级别：**当两个属于同一安全区的接口具有不同的安全级别时，防火墙将从框架上保证来自安全级别高的接口的会话能够自由访问从安全级别低的接口出去的连接，而无须添加任何防火墙策略，而来自安全级别低的接口的会话即使防火墙的策略允许也不能访问从安全级别高的接口出去的连接。当两个属于同一安全区的接口具有相同的安全级别时，需要添加防火墙的访问控制策略才能访问。

**物理接口还可以提供 VLAN 功能**（依具体产品型号而定，一般低端产品不具备该功能）。



新建VLAN接口	
接口名	<input type="text"/>
VLAN ID	<input type="text"/>
接口类型	非广域网
工作模式	<input checked="" type="radio"/> ROUTE <input type="radio"/> NAT
IP地址	<input type="text"/>
网络掩码	<input type="text"/>
访问许可	<input checked="" type="checkbox"/> SNMP <input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> SSH <input checked="" type="checkbox"/> TELNET
安全级别	0
最大传输单元	1500
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 7-19:VLAN 接口设置界面

**接口可以添加多个二级 IP。**



接口

**新建接口E1二级IP**

IP地址: 0.0.0.0

网络掩码: 255.255.255.0

确定 取消

图 7-20: 接口二级 IP 设置界面

## ◇ 路由

Anysec 设备提供静态路由和策略路由两种路由管理方式。出厂默认的配置下，Anysec 设备路由表只包含直连路由信息。用户可以通过定义其他的静态路由在路由表中添加路由信息。

### ● 静态路由

下图为静态路由界面，用户可以查看设备当前的系统路由表，也可以通过添加按钮新增静态路由。



ID	目的IP	子网掩码	网关地址	跳数	接口	编辑
1	192.168.118.1	255.255.255.255	0.0.0.0	0	ppsec0	
2	116.204.100.1	255.255.255.255	0.0.0.0	0	ppp0	
3	192.168.0.99	255.255.255.255	0.0.0.0	0	ppsec1	
4	218.17.59.1	255.255.255.255	0.0.0.0	0	ppp1	
5	192.168.118.0	255.255.255.0	0.0.0.0	0	ppsec0	
6	192.168.1.0	255.255.255.0	0.0.0.0	0	E1	
7	192.168.0.0	255.255.255.0	0.0.0.0	0	ppsec1	
8	192.168.59.0	255.255.255.0	0.0.0.0	0	E0	
9	127.0.0.0	255.0.0.0	0.0.0.0	0	ipsec	
10	0.0.0.0	0.0.0.0	116.204.100.1	0	ppp0	
11	0.0.0.0	0.0.0.0	218.17.59.1	0	ppp1	

图 7-21: 静态路由设置界面

## ● 策略路由

每当一个数据包到达 Anysec 设备中任何一个接口时, Anysec 设备将通过使用该数据包包头含有的源 IP 地址做逆向查询以识别该数据包是否在合法的接口接收的。

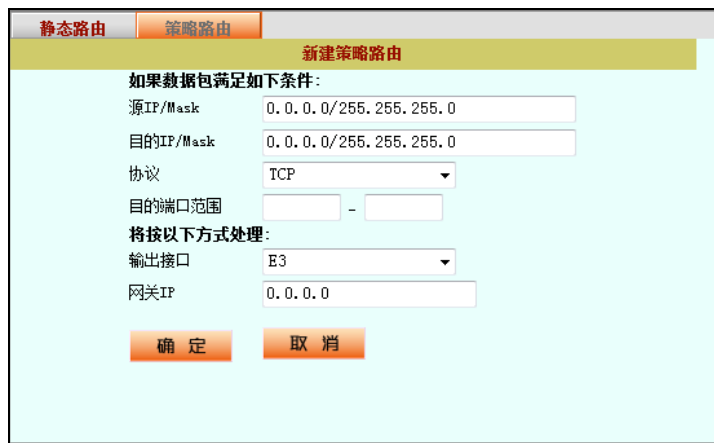
如果 Anysec 设备通过接收该数据包的接口不能与计算机的源 IP 地址通信, 那么 Anysec 将丢弃该数据包。

如果目标地址与本地地址能够匹配 (并且本地配置允许数据包的传输), 那么 Anysec 设备将数据包传送到本地网络中。

如果数据包的传输目的地是其他的网络, Anysec 设备根据路由策略或存储在 Anysec 转发路由表中的信息将把数据包转送在下一站中继路由。

当设置了路由策略并且数据包到达 Anysec 设备时, Anysec 设备根据策略路由表逐次查看并试图找到与该数据包相匹配的策略。如果发现匹配信息并且策略中包含了足够的信息路由数据包 (必须注明下一站路由的 IP 地址以及将数据包转发的接口), Anysec 设备将使用策略中的信息路由数据包。如果没有与数据包相匹配的策略, Anysec 设备将使用路由表路由数据包。

下图为添加策略路由的操作界面。



新建策略路由	
如果数据包满足如下条件:	
源IP/Mask	0.0.0.0/255.255.255.0
目的IP/Mask	0.0.0.0/255.255.255.0
协议	TCP
目的端口范围	-
将按以下方式处理:	
输出接口	E3
网关IP	0.0.0.0
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 7-22: 新建策略路由设置界面

◇ DNS

● DNS

Anysec 设备的 DNS 配置。一般该 DNS 服务器信息由 ISP 提供。



DNS	SecROS简域	DDNS
<b>DNS设置</b>		
主DNS服务器:	<input type="text" value="211.162.78.1"/>	
从DNS服务器:	<input type="text" value="211.162.78.2"/>	
<input type="button" value="确定"/>		

图 7-23: DNS 设置界面

注意：各地 DNS 并不相同，请查询当地 ISP 运营商提供的 DNS 服务器信息。

● SecROS 简域

中科网威与 ISP 运营商合作，为客户提供的自主认证平台，非固定 IP 用户推荐使用该寻址模式。

设备寻址更加稳定、快速。该功能仅支持拥有点点通策略平台的设备。



DNS	SecROS简域	DDNS
<b>SecROS简域设置</b>		
简域名:	<input type="text" value="lǎnzhōuhu"/>	
密码:	<input type="password" value="*****"/>	
确认密码:	<input type="password" value="*****"/>	
服务状态:	<input type="checkbox"/>	
<input type="button" value="确定"/>		

图 7-24:SecROS 简域设置界面

(默认出厂配置完成, 如果因特殊原因导致丢失该信息, 请联系中科网威工程师重发配置信息)

### ● DDNS

Anysec 支持 DDNS (动态域名) 功能。

下图为添加一个动态域名的操作界面。



图 7-25:新建 DDNS 动态域名界面

目前 Anysec 设备只支持 3322 的动态域名服务, 您可以通过 <http://www.3322.org> 进行 DDNS (动态域名) 免费申请, 将相关信息输入以后, 在相关广域网接口的配置信息中选择您申请的 DDNS 即可, 这样您就随时都能通过 DDNS 来对设备进行访问了。

### ◇ DHCP

DHCP 协议可以使 PC 自动获取分配的 IP 地址。或者也可以获取默认的网关与 DNS 服务器设置。一个 Anysec 物理接口或 VLAN 子接口能够提供以下 DHCP 服务:

- 1、为常规以太网连接提供常规的 DHCP 服务器服务。
- 2、为 IPSEC (VPN) 连接提供 IPSEC DHCP 服务器服务。
- 3、为常规以太网或 IPSEC 连接提供 DHCP 中继服务。

对于相同类型的连接 (常规或 IPSEC), 一个接口不能既提供 DHCP 服务器服务又提供中继代理服务。

用户可以对任何 Anysec 接口配置 DHCP 服务器功能。DHCP 服务器对与该接口连接的网络中的主机动态分配 IP 地址。在主机上必须配置使用 DHCP 自动获取分配的 IP 地址。

如果一个接口通过路由器与多个网络连接，用户可以对每个网络添加一个 DHCP 服务器。每个 DHCP 服务器的 IP 地址范围必须与网络地址范围像匹配。路由器必须配置使用 DHCP 中继代理。

Anysec 接口可以配置作为 DHCP 中继代理。接口将 DHCP 用户端的 DHCP 请求转发到外部 DHCP 服务器并将响应返回到 DHCP 用户。DHCP 服务器必须具有适当的路由，以便返回到 DHCP 用户的响应数据包能够到达 Anysec 设备。

## ● 服务器

下图为添加一个 DHCP 服务器的操作界面。



图 7-26: 新建 DHCP 服务器界面

域名、DNS 服务器以及 WIS 服务器属于可选输入，您可以依据您的具体情况进行填写。

## ● IP/MAC 绑定

该功能可以为具体的用户保留 IP 地址

根据用户设备 MAC 地址与连接类型、常规以太网连接或 IPSEC 连接；用户可

以为具体的用户保留一个 IP 地址。DHCP 服务器总是将保留的地址分配给该用户。



服务器 | IP/MAC绑定 | 分配列表 | DHCP中继

新建DHCP IP/MAC绑定

名称

IP地址

MAC地址

确定 取消

图 7-27:新建 DHCP IP/MAC 绑定界面

- 分配列表

显示当前已分配的 IP 地址信息及过期时间等。



ID	MAC地址	IP地址	过期时间	状态
1	00:1B:4E:1E:72:96	192.168.59.100	0 days 07:59:44	

图 7-28:分配列表界面

- DHCP 中继

针对具有 DHCP 服务器的客户，提供 DHCP 中继服务。



服务器 | IP/MAC绑定 | 分配列表 | DHCP中继

新建DHCP中继服务

服务名

DHCP中继接口

DHCP服务器IP

状态

确定 取消



图 7-29:新建 DHCP 中继服务界面

## ◇ 会话

Anysec 设备提供会话和 ARP 查看,能够实时查看系统当前的网络会话状态、ARP 信息和高级选项。

### ● 会话

显示当前设备的网络会话情况。



ID	协议	源 IP	源端口	目的 IP	目的端口	状态	失效 (秒)	操作
1	tcp	10.0.0.2	52212	192.168.59.1	8080	TIME_WAIT	115	[图标]
2	tcp	10.0.0.2	52212	192.168.59.1	8080	ESTABLISHED	3594	[图标]
3	tcp	10.0.0.2	52205	192.168.59.1	8080	TIME_WAIT	115	[图标]
4	tcp	10.0.0.2	52197	192.168.59.1	8080	TIME_WAIT	114	[图标]
5	tcp	10.0.0.2	52219	192.168.59.1	8080	TIME_WAIT	115	[图标]
6	tcp	10.0.0.2	52204	192.168.59.1	8080	TIME_WAIT	115	[图标]
7	udp	211.182.101.114	14750	118.204.100.250	4455		14	[图标]
8	tcp	10.0.0.2	52190	192.168.59.1	8080	TIME_WAIT	114	[图标]
9	tcp	10.0.0.2	52216	192.168.59.1	8080	TIME_WAIT	115	[图标]
10	tcp	10.0.0.2	52193	192.168.59.1	8080	TIME_WAIT	115	[图标]

图 7-30:当前设备的网络会话界面

### ● ARP

显示与当前设备接口连接的 ARP 信息,您可以通过通过“绑定状态”来将 PC 的 IP 和 MAC 进行绑定以抵御 Anysec 设备免受 ARP 欺骗攻击。注:当 PC 受到内网 ARP 攻击导致无法和 Anysec 设备通信时,请在您的 PC 上安装防 ARP 欺骗的杀毒软件来解决。



图 7-31: 当前设备接口连接的 ARP 信息界面

### ● 高级选项

对 Anysec 设备的网络会话超时以及 TCP 会话数和 SYN 洪水攻击进行设置。

默认情况下 Anysec 设备的 TCP 会话的超时时间为 3600 秒;UDP 会话的超时时间为 30 秒; ICMP 会话的超时时间为 1 秒。

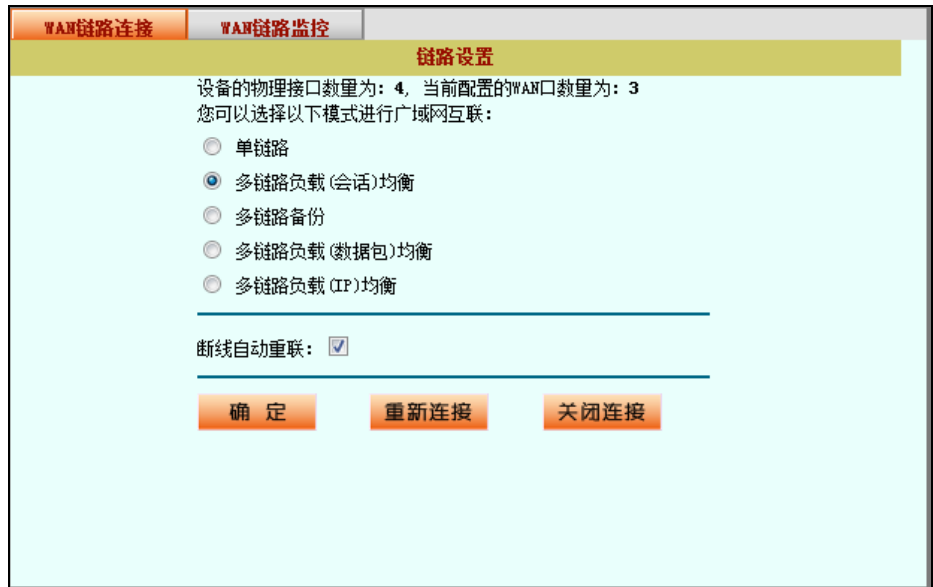
IP 最大 TCP 会话数限制: 对 PC 的并发 TCP 连接进行限制, 该功能能够在一定程度上缓解 P2P 下载所造成的带宽滥用情况。

TCPMSS 设置:

入侵检测与防范: \_\_\_\_\_



图 7-32: 高级选项设置界面



## 链路

Anysec 设备提供链路管理及监控，支持多链路上网（低端设备无该功能）。

- WAN 链路管理

图 7-33: WAN 链路设置界面

当您的设备存在多 WAN 口配置时，您需要选择广域网联网模式为“多链路负载均衡”或“多链路负载均衡及带宽叠加”，否则 Anysec 设备将按“单链路”进行联网处理。

- WAN 链路监控



WAN 接口名	联网方式	当前接口 链路状态	IP	PVID	设备 MAC	链路时间	接入时间
1	PPPoE	ppp	118.200.100.100	118.200.100.1	7788007788000000	7788007788000000	2012.01.20 9
2	PPPoE	ppp	118.200.100.100	118.200.100.1	8800007788000000	8800007788000000	2012.01.20 9
3	静态 IP	IP	192.168.1.111	11111	9999999999999999	9999999999999999	2012.01.20 9

图 7-34: WAN 链路监控界面

对 WAN 联网情况进行监控，能直观的显示接口的 WAN 连网方式，当前 IP 地址、网关地址、已发送和已接收的数据包及字节数以及改接口接入 Internet 的时间。

## ② 用户管理

### 配置用户验证

Anysec 设备验证设置是控制用户组的访问，但是创建用户组并不是配置验证的第一步。用户可以依据以下步骤配置用户验证设置：

如需要外部验证，可以配置 RADIUS、LDAP、POP3 或 TACACS 服务器。

进入“用户管理”->“用户”，可以配置本地用户验证。对于每个用户，可以设置通过 Anysec 设备、RADIUS 服务器、LDAP 服务器、POP3 服务器或 TACACS 服务器校验密码。

### ◇ 用户

进入用户管理->用户，添加用户名称并配置验证。

下图为添加用户的操作界面。



图 7-35: 新建认证用户界面

认证方式里面，支持多种认证，密码表示本地认证，其余部分均属于外部认证，需配置好对应的认证服务器。

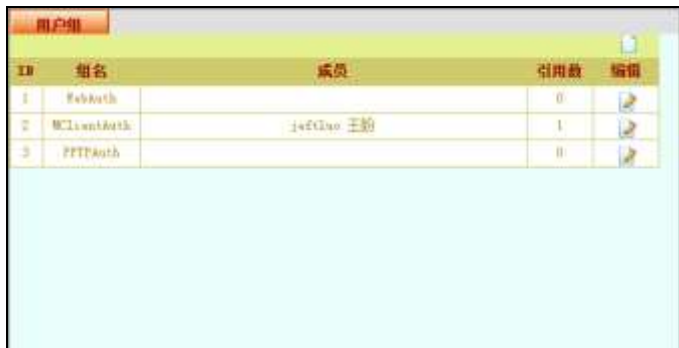
Web 认证选项是用于上网认证的身份识别，可以绑定 IP 和 MAC 地址。

远程客户端接入指定 IP 是用于移动客户端接入的，如果填写了 IP 地址，则使用该用户接入的远程客户端会分配指定的 IP。

状态表示该新建用户是否被激活启用。

## ◇ 用户组

一个用户组是一个或多个用户的集合。Anysec 设备出厂默认有三组用户组。






ID	组名	成员	引用数	编辑
1	WebAuth		0	
2	MClientAuth	jeftlao 王勃	1	
3	PPTPAuth		0	

图 7-36: 用户组显示界面

**PPTPAuth 用户组：**用于提供 PPTP 远程接入身份验证的用户组类型。

**WebAuth 用户组：**用于提供上网认证的身份验证的用户组类型。（默认组，不可改变）

**MClientAuth 用户组：**用于提供移动客户端远程接入身份验证的用户组类型。

注意：您在启用 PPTP 服务和移动客户端服务的时候可以选择“PPTPAuth”认证用户组和“MClientAuth”用户组，但也可以新建其他用户组，并将认证用户选入该用户组，在相关应用中引用就可以了。

WebAuth 用户组有点特殊，当您的防火墙策略需要用户进行 Web 认证上网的时候，请将用户加入该用户组，否则用户将无法认证上网。



图 7-37: 编辑用户组界面

#### ◇ RADIUS

对外部 Radius 服务器信息进行配置。

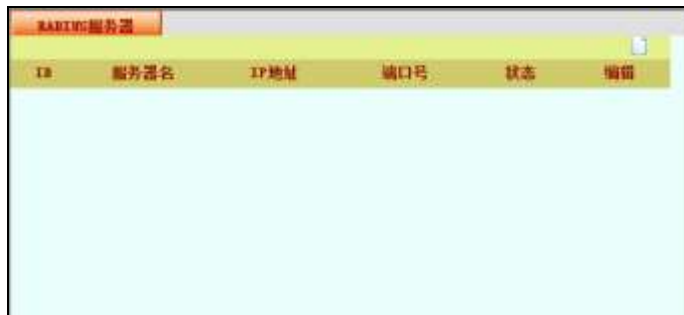


图 7-38: 外部 Radius 服务器信息界面

新建 Radius 认证服务器:



图 7-39：新建 Radius 认证服务器界面

- ◇ LDAP（略）
- ◇ POP3（略）
- ◇ TACACS+（略）

服务器设置方法类似，如有疑问，请致电中科网威技术工程师：0755-83658229。

## 🔍 防火墙

本章用于描述 Anysec 设备的防火墙功能，

Anysec 设备提供网络安全的核心功能都是围绕防火墙展开的，其上网行为管理和网络监控功能均需与防火墙策略的配合，管理员定义上网行为管理策略和网络监控策略，必须将其在防火墙策略中引用才能生效。

### ◇ 策略

防火墙策略控制所有通过 Anysec 设备的通信流量。添加防火墙策略控制 Anysec 安全区之间的连接与流量。

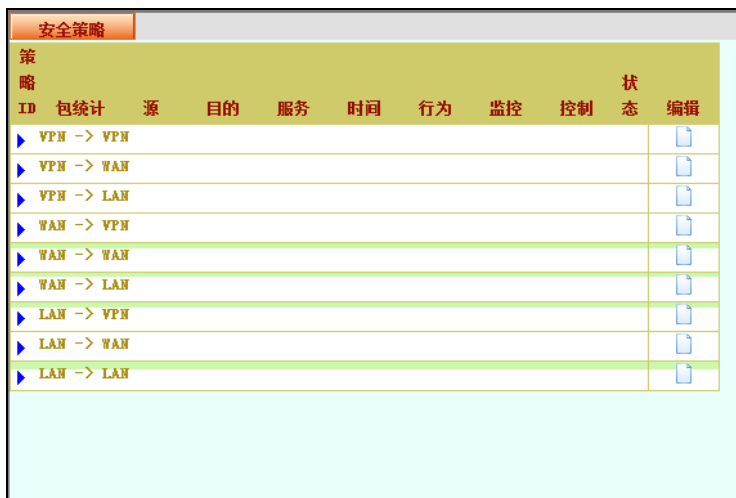
防火墙策略是 Anysec 设备决定如何处理连接请求的指令。当防火墙收到



一个数据包发出的连接请求时，Anysec 提取这个数据包的源地址、目的地址和服务（端口号）进行分析。

对于通过 Anysec 设备传输数据包，必须在 Anysec 设备上添加一个与该数据包源地址、目的地址和服务相匹配的防火墙策略。该策略指导防火墙如何处理这个数据包。处理方式可以是允许连接、拒绝连接、在连接前要求认证，或将数据包作为 IPSec VPN 包处理。您也可以对防火墙策略添加日志记录，配置 Anysec 设备记录对所有连接使用的策略。防火墙通过对策略列表的顺序搜索查找匹配策略。Anysec 设备的默认的策略是拒绝所有的连接。策略选项是通过创建或编辑防火墙策略时配置的。根据您所选择的不同的控制方式，将呈现不同的策略选项。

下图为防火墙策略列表的界面












安全策略											
策略	ID	包统计	源	目的	服务	时间	行为	监控	控制	状态	编辑
	▶										
	▶										
	▶										
	▶										
	▶										
	▶										
	▶										
	▶										
	▶										

图 7-40：防火墙安全策略列表界面

### 添加防火墙策略：

点击插入策略按钮，可以添加一条安全策略。

安全策略的匹配条件包含了：

**来源、流入接口、目的、流出接口、服务、时间、行为、控制、监控、流量控制、日志、状态。**

- 1、来源和目的对应防火墙地址；
- 2、服务对应防火墙服务；

- 3、时间对应防火墙时间；
- 4、行为对应行为管理的策略；
- 5、控制包括运行、拒绝和认证，其中认证是指上网认证；
- 6、监控对于网络监控的策略；
- 7、流量控制包含启用和不启用两种状态；
- 8、日志标明是否记录数据包；
- 9、状态用于表明策略是否生效；

下图为插入安全策略的操作界面。



插入安全策略	
来源	ANY
流入接口	ANY
目的	ANY
流出接口	ANY
服务	ANY
时间	ANY
行为	NONE
控制	ALLOW
监控	NONE
流量控制	disable
日志	<input type="checkbox"/>
状态	<input checked="" type="checkbox"/>

图 7-41：插入安全策略设置界面

#### ◇ 地址

用户可以根据需要添加、编辑以及删除防火墙地址。防火墙地址将被添加到防火墙策略的源以及目标地址字段。添加到防火墙策略中的地址是用来与 Anysec 设备接收到数据包的源以及目标地址相匹配的。

##### ● IP 掩码

一个防火墙地址可以是：

- 1、单个计算机的 IP 地址（例如，192.168.0.69/255.255.255.255）。
- 2、一个子网的 IP 地址（例如，class C 子网的地址 192.168.0.0/255.255.255.0）。

3、0.0.0.0/0.0.0.0 表示所有可能的 IP 地址。

所添加的 IP 地址对应的掩码。例如：

- 单个计算机 IP 地址的掩码应该为 255.255.255.255
- Class A 子网的掩码应该为 255.0.0.0
- Class B 子网的掩码应该为 255.255.0.0
- Class C 子网的掩码应该为 255.255.255.0
- 所有地址的掩码应该为 0.0.0.0

**注意：**IP 地址为 0.0.0.0 与掩码为 255.255.255.255 不是有效的防火墙地址。

下图为新建 IP 掩码的操作界面。

IP掩码	IP范围	地址组
新建IP掩码		
名称		
IP地址	0.0.0.0	
网络掩码	255.255.255.0	
状态	<input checked="" type="checkbox"/>	
确定		取消

图 7-42:新建 IP 掩码设置界面

### ● IP 范围

IP 范围能够定义一段 IP 地址（如：192.168.0.1 到 192.168.0.10）



图 7-42:新建 IP 范围界面

- **地址组**

地址组为 IP 掩码和 IP 范围对象的集合。



图 7-43:新建地址组界面

## ◇ 服务

设置服务识别防火墙接收或拒绝的通信会话类型。用户可以在策略中添加任何预先定义的服务。用户也可以创建用户服务或在服务组中添加服务。

### ● 预定义

下图为查看预定义的服务列表。Anysec 系统设置的预定义服务目前有二十余种，基本上包含了用户使用率比较高的服务对象。

预定义		自定义	服务组		
ID	名称		详情	引用数	
1	FTP		tcp/21	0	
2	HTTP		tcp/80	0	
3	SSH		tcp/22	0	
4	SMTP		tcp/25	0	
5	MSN		tcp/1883	0	
6	LDAP		tcp/389	0	
7	RDP		tcp/3389	0	
8	POP		tcp/110	0	
9	RADIUS		tcp/1812-1813	0	
10	STUN		udp/514	0	
11	TCP		tcp/1-65535	0	
12	MYSQL		tcp/3306	0	
13	TFTP		udp/69	0	
14	IPsec		comp/0	0	
15	HTTP		tcp/80	0	

图 7-44: 预定义服务列表界面

- **自定义**

当您的应用服务在自定义服务列表中找到时，您就需要在自定义服务对象功能中新建了，以下为新建自定义服务的界面：



新建自定义服务				
服务名: <input type="text"/>				
协议	目的端口		源端口	
	起始	结束	起始	结束
<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<input type="text"/>	<input type="text"/>	1	65535
状态: <input checked="" type="checkbox"/>				
<input type="button" value="确定"/> <input type="button" value="取消"/>				

图 7-45：新建自定义服务界面

- **服务组**

服务组为预定义服务和自定义服务的集合。



新建服务组	
组名: <input type="text"/>	
可用服务: <ul style="list-style-type: none"> <li>VNC</li> <li>UDP</li> <li>POP</li> <li>MSNGL</li> <li>RSH</li> <li>LDAP</li> <li>DHCP</li> <li>BGP</li> </ul>	已选服务: <div style="border: 1px solid gray; height: 100px; width: 100%;"></div>
状态: <input checked="" type="checkbox"/>	
<input type="button" value="确定"/> <input type="button" value="取消"/>	

图 7-46：新建服务组界面

### ◇ 时间

设置时间表控制激活与中止策略的时间。用户可以设置固定时间表或循环时间表。使用固定时间表创建一项策略在指定的时间段内生效。循环时间表每周进行一个循环。用户可以使用循环时间表设置一项策略只在指定的一天中循环几次或一星期中某些天之内生效。

#### ● 一次性时间

下图为新建一次性时间的操作界面



新建一次性时间					
名称					
开始	年份	月份	日期	小时	分钟
	2010	01	01	00	00
停止	年份	月份	日期	小时	分钟
	2010	01	01	00	00
状态	<input checked="" type="checkbox"/>				
确定			取消		
注：开始时间应大于启用时间并小于停止时间。					

图 7-47：新建一次性时间界面

#### ● 循环时间

下图为新建循环时间的操作界面



图 7-48: 新建循环时间界面

## ◇ 地址转换

### ● 虚拟 IP (目的地址转换)

使用虚拟 IP 能够访问源网络中被 NAT (network address translation: 网络地址转换) 安全策略隐藏的目标网络的 IP 地址。例如, 您可以在外部网络 Anysec 设备接口添加一个虚拟 IP 地址, 那么外部接口 就可以对实际上与 DMZ 或内部网络中服务器连接的用户发出的请求作出回应。

下图为新建虚拟 IP 服务的操作界面。



图 7-49: 预定义服务列表界面



- 源地址转换

下图为新建源地址转换的操作界面。



图 7-50：新建源地址转换设置界面

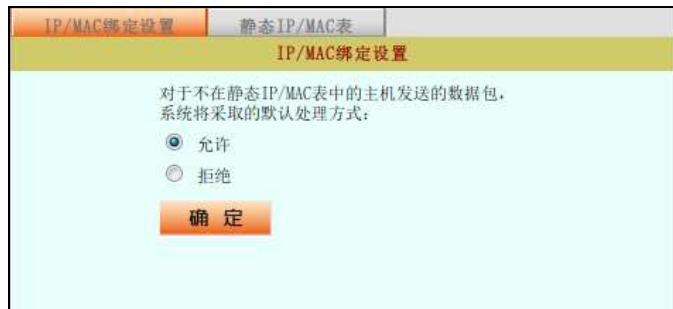
- ◇ IP/MAC 绑定

- IP/MAC 地址绑定设置

对于不在静态 IP/MAC 表中的内网 PC 数据做如何处理，处理方式包括：

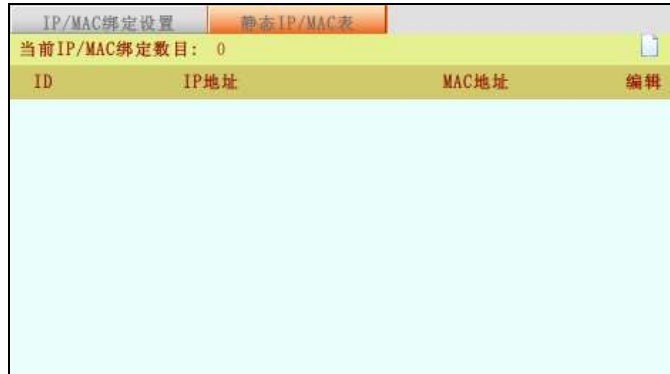
允许：仅允许不在静态 IP/MAC 表中的 PC 机发送数据包，静态 IP/MAC 表中的 PC 机发送的数据包将被网关设备拒绝；

拒绝：仅允许在静态 IP/MAC 表中的 PC 机发送数据包，不在静态 IP/MAC 表中的 PC 机发送的数据包将被网关设备拒绝。



- **静态 IP/MAC 表**

对内网 PC 机进行 IP 地址和网卡 MAC 地址绑定，点击右上角“新建”即可添加。



ID	IP地址	MAC地址	编辑
----	------	-------	----

## VPN 管理

Anysec 设备提供了多种 VPN 技术服务，在提供标准的 PPTP/IPSEC VPN 服务的同时，也提供了个性化的，针对企业应用的点点通智能 VPN；针对移动办公应用的 SSL VPN 和移动客户端服务。

### ◆ 点点通

点点通是 Anysec 设备针对企业用户推出的个性化的智能 VPN 解决方案。主要分为两个部分。

- ✓ 设备隧道管理（终端支持）
- ✓ 隧道连接管理（平台支持）

### ◆ 设备隧道管理

#### ● 配置

如何配置一个隧道： 点击 VPN 管理->点点通->配置菜单，可以看到下面的图示。



The screenshot shows a web-based configuration interface for a VPN tunnel. At the top, there are navigation tabs: "配置" (Configuration), "隧道监控" (Tunnel Monitoring), "设备管理" (Device Management), "连接管理" (Connection Management), and "在线设备" (Online Devices). The "配置" tab is selected, and the sub-section "设备配置" (Device Configuration) is active. The configuration form includes the following fields and options:

- 设备名 (Device Name): device3
- 设备ID (Device ID): 1002
- 通讯密码 (Communication Password): masked with dots
- 隧道策略寻址方式 (Tunnel Policy Addressing Method):
  - 通过公网IP或域名寻址 (Via public IP or domain name)
  - 通过SecROS网络平台寻址 (Via SecROS network platform)
- 策略中心地址 (Policy Center Address): myspace
- 上级策略中心地址 (Superior Policy Center Address): empty field with a checkbox
- 现在激活 (Activate Now): checkbox
- 确定 (Confirm) button

图 7-51：VPN 管理下设备配置界面

设备名、设备 ID、通讯密码是在隧道连接管理定义的，设备名和设备 ID 用于表示一个拥有点点通隧道的 Anysec 设备身份，通讯密码是 Anysec 设备到隧道连接管理平台的认证密码。

策略中心地址是隧道连接管理平台的地址，可以是 IP 地址，也可以是一个域名。

现在激活表示点点通隧道的状态是否生效。

- **隧道监控**

如何监控隧道状态：

点击 VPN 管理->点点通->隧道监控菜单，可以查看点点通隧道的状态。

下图为点点通隧道的监控界面。您可以点击“测试”按钮测试当前隧道是否正常连通。

图 7-52：VPN 管理下隧道监控界面

- **隧道连接管理**

隧道连接管理是点点通平台的一个重要功能，用于定义点点通设备和隧道策略。

- **设备管理**

如何定义一个点点通设备：

点击 VPN 管理->点点通->设备管理页面里面的新建按钮，可以新建一个点点通设备对象。

下图为新建设备的界面。

配置	隧道监控	设备管理	连接管理	在线设备
<b>新建设备</b>				
设备名	<input type="text" value="研发中心"/>			
设备ID	<input type="text" value="1003"/>			
通讯密码	<input type="password" value="●●●●●"/>			
联网模式	动态公网IP或NAT设备后 ▾			
内网口IP	<input type="text" value="192.168.0.99"/>			
在线生存期	<input type="text" value="300"/> ( 120-3600 秒)			
联系人	<input type="text" value="王盼"/>			
电话	<input type="text" value="13713867534"/>			
备注	<input type="text" value="研发中心"/>			
<input type="button" value="确定"/>		<input type="button" value="取消"/>		

图 7-53: VPN 管理下新建设备配置界面

设备名与设备 ID 表示一个点对点设备的身份，其中设备 ID 和设备名都必须唯一。

通讯密码用于设备到平台的身份认证。

联网模式表明该设备的上网方式。

内网 IP 是设备的内网口 IP 地址，也是用于建立隧道的内网地址。

下图为设备列表界面。



图 7-54: VPN 管理下设备列表界面

新建设备成功后，您还需要对该设备的隧道子网进行定义，请点击“隧道子网定义”图标，按照实际情况将隧道子网一一加入即可。

下图为隧道子网定义界面：



图 7-55: VPN 管理下设备隧道子网配置界面

### ● 连接管理

如何定义一条隧道策略：

点击 VPN 管理->点点通->连接管理菜单，选择一个设备，点击“修改连接策略”按钮，将出现下图所示的界面。



图 7-56: VPN 管理下新建连接策略设置界面

从可互联设备列表中选择需要建立隧道的设备到已选设备列表即可。

当需要互联的两台设备都处于 NAT 环境中如何处理：

点击 VPN 管理->点点通->连接管理菜单，选择其中一台设备，点击“修改连接属性”按钮，在出现的连接列表中选择“修改连接属性”按钮，将连接方式由“直接连接”改为“第三方中转”，并选择相应的中转设备即可。

### ● 在线设备

如何查看点点通隧道与设备状态：

点击 VPN 管理->点点通->在线设备菜单，可以查看在平台内定义的所有设备的在线状态和隧道状态。

下图为在线设备界面。



ID	设备名	设备ID	认证IP	WAN口	更新时间	在线生存期 (秒)	当前状态	操作
1	device3	1002	219.139.88.40	否	Fri Jan 22 09:37:10 2010	300	●	🔍 🗑️ 🔄 🛠️
2	北京办事处	1006	114.117.18.45	否	Fri Jan 22 09:36:26 2010	300	●	🔍 🗑️ 🔄 🛠️

图 7-57: VPN 管理下在线设备显示界面

您可以点击“设备详情”按钮查看当前设备的基本情况，例如设备名、设备ID、设备型号及类型、软硬件版本、认证IP地址以及WAN链路情况。



设备 device3 详情	
设备名	device3
设备ID	1002
设备型号	38100
设备类型	380
软件版本	20100120-20100120
硬件版本	20100101-380
认证IP	219.139.88.40
联网模式	动态公网IP和WAN设备后
<input type="button" value="确定"/>	

图 7-58: VPN 管理下在线设备详情界面

您也可以点击“隧道状态”查看与该设备互联的所有隧道情况。



配置	隧道管理	设备管理	连接管理	在线设备
ID	隧道名	连接方式	中转设备名	隧道状态
1	davinci-北信点系统	直连设备		

图 7-59：VPN 管理下在线设备隧道状态界面

您还可以点击“在线设备控制”按钮，对设备进行简单控制：

配置	隧道管理	设备管理	连接管理	在线设备
在线设备：davinci3 控制				
设备维护				<input type="radio"/> 设备重启 <input checked="" type="radio"/> 保存当前运行配置
广域网				<input type="radio"/> 关闭广域网连接 <input type="radio"/> 重置广域网
VPN白名单				<input type="radio"/> 重新同步连接策略 <input type="radio"/> 重建所有隧道 <input type="radio"/> 保存当前隧道策略
防火墙				<input type="radio"/> 开启放行 <input type="radio"/> 关闭转发
<input type="button" value="确定"/> <input type="button" value="取消"/>				

图 7-60：VPN 管理下在线设备控制设置界面

## ◇ PPTP

Anysec 设备支持点对点通道协议进行两个对等体之间的 PPP 通讯流量。Windows 或 Linux PPTP 用户可以与配置作为 PPTP 服务器的 Anysec 设备建立一个 PPTP 通道。用户也可以配置 Anysec 设置将 PPTP 数据包转送到置于 Anysec 设备之后的网络中的 PPTP 服务器。PPTP 配置只适用于 NAT/路由模式。当前 PPTP 与 L2TP 会话的最大数量为 254。起始与结束的 IP 必须在相同的 24bit 的子网中，例如 x.x.x.1-x.x.x.254。

### ● 参数配置

如何设置 PPTP 服务：

点击 VPN 管理->PPTP->参数配置菜单，可以配置 PPTP 服务，如下图所示。



图 7-61：PPTP 设置界面

起始 IP 地址和最大接入数定义了 PPTP 接入后分配的 IP 范围和 PPTP 服务的最大连接数目。

认证用户组可以选择 PPTPAuth 认证用户组，也可以选择其他用户组。服务状态表明 PPTP 服务是否开启。

### ● 在线用户

显示当前通过 PPTP 方式接入网络的在线用户情况。

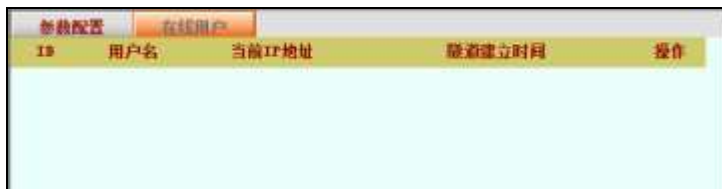


图 7-62：PPTP 在线用户显示界面

## ◇ IPSEC

Anysec 设备支持 IPSEC VPN，提供了标准的 IKE/IPSEC 服务，能够与第三方设备互联，同时还提供了手工指定 SPI 方式建立 IPSEC 隧道的快速服务和隧道查看功能。

### 关于 IPSEC 接口模式：

在用户定义 IPSEC 隧道的时候，需要将设备的 IPSEC 接口绑定到内网口上，默认出厂配置里面 IPSEC 接口的 IP 是 127.0.0.1。

### ● 手动模式

手动模式是 Anysec 设备提供的一种快速建立 IPSEC 隧道的特殊功能，省去了 IKE 协商，直接输入 IPSEC 隧道建立的所需参数。

下图为添加一条手动隧道的操作界面。



图 7-63：新建手动模式隧道配置界面

- **如何与第三方设备建立 IPSEC VPN**

Anysec 设备支持与第三方 VPN 设备建立 IPSEC VPN。需要建立 IPSEC VPN 的双方设备采用 IKE 密钥交换协议进行身份认证和密钥协商, IKE 协议分为 2 个阶段。

- **IKE-阶段 1**

下图为新建 IKE-阶段 1 的操作界面。

手动模式	IKE-阶段1	IKE-阶段2	IKE模式	隧道监视器
<b>新建IKE-阶段1</b>				
阶段1名称	home			
远程网关类型	静态IP			
IP地址	123.23.112.21			
模式	<input checked="" type="radio"/> 主模式 <input type="radio"/> 野蛮模式			
认证方式	预共享密钥			
预共享密钥	●●●●●●			
<b>高级选项</b>	(Nat Traversal, XAUTH, DPD)			
算法提议	<input checked="" type="checkbox"/>			
加密算法	3DES_CBC			
认证算法	MD5			
DH算法	MODP1024			
密钥生存期	28800		(120-86400 秒)	
对端ID	wangpan@anysec.com		(可选)	
本端ID	jefl@anysec.com		(可选)	
NAT-T支持	<input checked="" type="checkbox"/>			
XAUTH	<input checked="" type="radio"/> 不启用 <input type="radio"/> 客户端 <input type="radio"/> 服务器端			
DPD支持	<input checked="" type="checkbox"/>			
<b>确定</b>		<b>取消</b>		

图 7-64：新建手动模式隧道阶段 1 配置界面

### ➤ 阶段一名称

用户在新建一个 IKE-阶段 1 配置的时候，需要为这个配置起一个名称，该名称必须在阶段 1 的所有配置中是唯一的。

### ➤ 远程网关类型

远程网关类型是描述对端设备的上网方式，可以是静态 IP 或者域名（也包括动态域名）。

### ➤ 模式

IKE 第一阶段协商支持 2 种模式，一种是主模式，一种是野蛮模式，请与需要建立隧道的设备保持相同模式。

### ➤ 认证方式

认证方式分为预共享密钥和证书认证两种方式，如果采用预共享密钥方式，则需要填入事先约定的密码，如果采用证书认证，则需选定本地设备证书和对端设备证书，证书在系统管理->证书功能里面配置。

### ➤ 算法

用户可以在 IKE 阶段一协商中选定需要使用的加密算法和认证算法。

### ➤ 密钥生存期

密钥生存期是指 IKE 阶段一协商出来的密钥的有效期，请与需要建立隧道的设备保持相同的密钥生存期。

### ➤ ID

ID 是表示本端和对端设备身份的一个标识，如果采用证书认证模式，则 ID 不需要另外填写，采用预共享密钥方式建立隧道，必须保证需要建立隧道的两个

设备的 ID 一致。

➤ **NAT-T 支持**

NAT-T 支持是用于穿越 NAT 设备的功能。

➤ **XAUTH**

XAUTH 认证是扩展认证，分为客户端和服务端，提供用户名/口令模式认证。

➤ **DPD 支持**

DPD 支持是心跳检测功能。

● **IKE-阶段 2**

下图为新建 IKE-阶段 2 的示例界面。

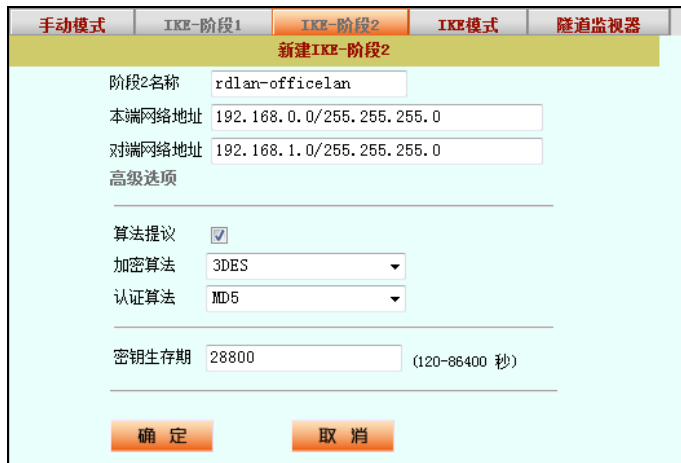


图 7-65：新建手动模式隧道阶段 2 配置界面

➤ **阶段 2 名称**

用户在新建一个 IKE-阶段 2 配置的时候，需要为这个配置起一个名称，该名称必须在阶段 2 的所有配置中是唯一的。

➤ **本端网络地址**

用于指定 VPN 隧道的本端网络信息。

➤ **对端网络地址**

用于指定 VPN 隧道的对端网络信息。

➤ **算法**

用于指定 IPSEC 隧道的加密算法和认证算法。

➤ **密钥生存期**

用于指定 IPSEC 隧道的密钥的有效期，请与需要建立隧道的设备保持相同的密钥生存期。

● **IKE 模式**

IKE 模式功能是在 IKE-阶段 1 和阶段 2 的基础上，创建 IPSEC VPN。如果设备处于防火墙后面或需要主动发起连接，则选中主动连接按钮。

下图为新建 IKE 模式隧道的示例界面。



手动模式	IKE-阶段1	IKE-阶段2	IKE模式	隧道监视器
<b>新建IKE模式隧道</b>				
隧道名	workvpn			
IKE-阶段1	home			
IKE-阶段2	rdlan-officelan			
主动连接	<input checked="" type="checkbox"/>			
确定		取消		

图 7-66: 新建 IKE 模式隧道配置界面

● **隧道监视器**

Anysec 设备提供 IPSEC VPN 隧道查看功能，可以查看手动隧道和 IKE 隧道。

下图为隧道监视器界面。



图 7-67：隧道监视器界面

#### ◇ SSL VPN

Anysec 设备提供 Web 转发保护的 SSL VPN 功能。

##### ● 参数配置

下图为 SSL VPN 设置的操作界面。

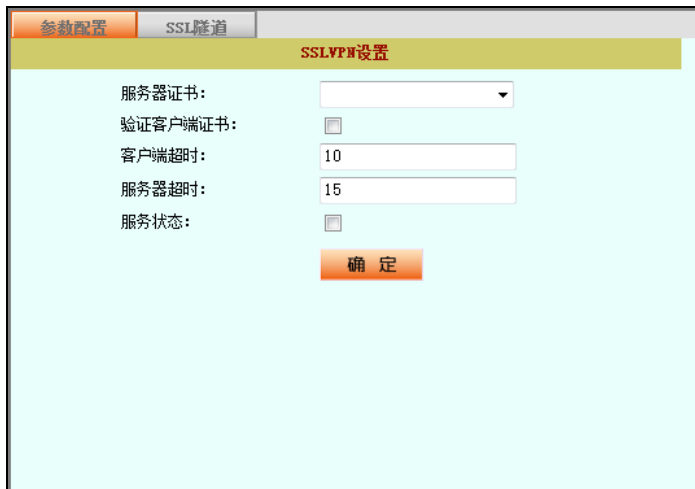


图 7-68：SSLVPN 设置界面



服务器证书是 Anysec SSL VPN 的设备证书，在系统管理的证书功能中加载或产生。

验证客户端证书是 SSL 的一项安全措施，可以要求设备验证客户端证书，确保用户身份。

客户端超时和服务器超时是用于维护 TCP 会话的时间参数，通常采用默认值。服务状态表示是否开启 SSL VPN 服务。

## ● 创建 SSL 隧道

下图为新建 SSL 隧道的操作界面。



图 7-69：新建 SSL 隧道配置界面

隧道名是 SSL VPN 的名称，必须保证唯一。

IP 地址是 SSL VPN 后台的 WEB 服务器的 IP 地址。

端口是 SSL VPN 后台的 WEB 服务器的端口。

用户组是用于指定身份认证的用户集合。

描述是用于表述该条 SSL VPN 的用途。

## ◇ 移动客户端

Anysec 设备的移动客户端是 Anysec 针对移动客户的接入需求,在 IPSEC VPN 技术的基础上优化推出的一个 IPSEC 隧道客户端功能,支持用户名/口令认证和证书认证。

移动客户端软件分为服务器端和客户端两大部分,其中服务器端的配置在 Anysec 设备上通过 WEB 或 CLI 来操作;客户端是一个运行在 Windows 系统下的应用程序,用户在使用前必须先运行移动客户端安装程序。

### ● 配置服务端

下图为移动客户端接入配置界面。

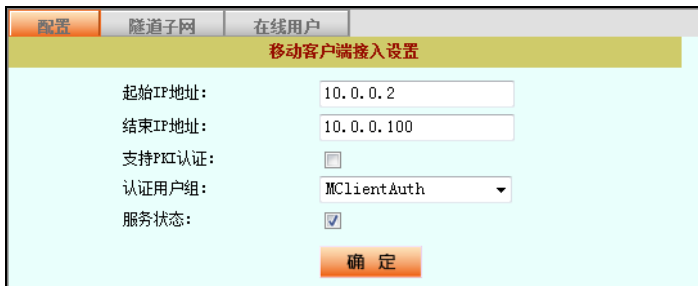


图 7-70：移动客户端接入设置界面

起始 IP 地址和结束 IP 地址用于定义分配给移动接入的用户的 IP 地址范围。

支持 PKI 认证是开启证书认证功能。

认证用户组是定义验证移动接入用户的身份识别的用户组。

服务状态是表明是否开启接入功能。

### ● 定义隧道子网

配置移动客户接入设置后，必须定义隧道子网，将 Anysec 设备非 WAN 接口的网段中，需要提供给移动客户访问的网段添加到隧道子网中，否则移动客户接入后还是无法访问内部网络。

下图为隧道子网的列表示例图。

ID	子网名	IP地址	掩码	状态	编辑
1	Client	192.168.89.0	255.255.255.0	开	

图 7-71：移动客户端隧道子网列表界面

下图为新建隧道子网示例图。



图 7-72：新建移动客户端隧道子网界面

### ● 在线用户

显示当前通过移动客户端接入的用户列表。通过该界面我们可以非常清楚的知道当前有哪些用户已经通过移动客户端软件或 Key 接入进来, 用户的 IP 地址以及隧道建立的时间等信息。

配置   隧道子网   <b>在线用户</b>				
ID	用户名	当前IP地址	隧道建立时间	编辑
1	王盼	10.0.0.2	Fri Jan 22 09:50:15 2010	

图 7-73：移动客户端在线用户显示界面

### ◇ 配置客户端

1、安装客户端后, 运行移动客户端程序会出现如下图所示的程序。



图 7-74: 移动客户端界面

2、点击“设置”按钮，出现高级设置窗口，可以查看已经建立的隧道，也可以建立新的隧道。



图 7-75: 移动客户端高级设置界面

3、点击“添加”按钮后，出现隧道配置框。



图 7-76：移动客户端隧道配置界面

- 隧道名称： →可任意填写。
- 寻址方式： 设备地址 →直接填写ANYSEC网关设备的固定IP或DDNS  
 动态域名；  
 策略中心 →填写点点通策略中心的固定IP或DDNS动态  
 域名统一寻址；  
 SecROS简域 →填写SecROS简域，通过中科网威ASN平台寻  
 址。
- 设备名称： →要与之建立VPN隧道的设备名称。
- 用户名： →在ANYSEC网关中开通的用户名。
- 口令： →在ANYSEC网关中开通的密码。
- 保存口令： →该设置勾选后能保存用户名和密码。
- 使用证书验证： →如果使用证书认证方式请勾选使用证书。

4、在高级设置窗口点击高级可以配置系统设置框，如下图所示。



图 7-77：移动客户端系统设置界面

系统设置框提供了断线重联和开机启动功能。

另外，还提供了虚拟网卡的管理功能，用户如果发现虚拟网卡出现问题，可以卸载或安装新的虚拟网卡。

## ☉ 行为管理

Anysec 行为管理是与防火墙功能相结合，向用户提供上网行为管理功能，用户在行为管理模块里面定义各种上网行为管理策略，必须在防火墙策略里面引用这些行为策略才能让设备进行上网行为管理。

上网管理策略包括了：

- DNS 策略
- 网页策略
- 文件策略
- 邮件策略

DNS 策略可以提供 DNS 屏蔽和 DNS 免屏蔽,通过 DNS 来控制用户对特定网站的访问控制。

网页策略是 URL 级的访问控制，粒度更细。

文件策略是使用文件后缀名作为控制条件的访问策略。

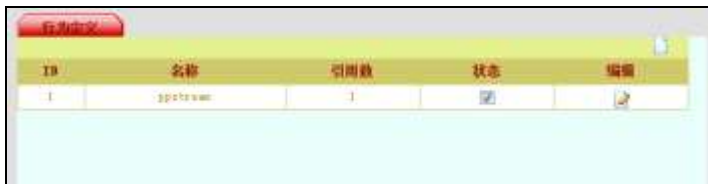
邮件审计 Anysec 针对邮件管理提供的一项高级功能，可以对邮件发送进行审计，可以制定免审计邮件和审计配置。

### ◇ 定义行为管理策略

点击行为管理->行为规则菜单，可以配置上网行为管理策略。

注意：您的行为管理策略需要在防火墙的访问控制中引用才能生效。

#### ● 查看行为定义



ID	名称	引用数	状态	编辑
1	http://www	1		

图 7-98：行为定义列表界面

**ID：**行为的序号。

**名称：**行为名称，被防火墙策略采用。



**引用数：**行为被引用的次数。

**状态：**行为是否被激活的状态。

- **新建行为定义**



图 7-99：新建行为属性设置界面

**名称：**指定新建行为的名称，用于防火墙策略里面的上网行为策略。

**状**

**态：**表明新建行为是否激活有效。

**DNS 控制：**包含了 DNS 行为控制，可以选择 DNS 定义里面的各种策略。

**网页控制：**包含了网页行为控制，可以选择网页定义里面的各种策略，可以控制 Web 邮件发送过滤，ActiveX 过滤和 Java Applet 过滤、Web 视频屏蔽。

**文件控制：**包含了文件行为控制，可以选择文件定义里面的各种策略。

**邮件控制：**可以启用发件审计功能。

**IM 控制、在线游戏、证券控制、P2P 视频控制、P2P 下载控制：**可以控制 QQ、MSN、

飞信、阿里旺旺、网易泡泡、雅虎通、Skype、WebQQ、QQ 游戏、联众游戏、中国游戏中心、浩方对战平台、网易泡泡游戏、边锋网络游戏、农场游戏、证券之星、大智慧、同花顺、龙卷风、网上赢家、钱龙、分析家、麒麟短线王、光大证券、广发证券、国信证券、招商证券、联合证券、国元证券、PPStream、PPlive、QQlive、快播 QVOD、UUSee、沸点电视、BT 下载、电驴、迅雷、超级旋风、百度下吧等常见应用行为。

#### ◇ DNS 定义

DNS 定义包括 DNS 屏蔽和 DNS 免屏蔽功能。

##### ● DNS 屏蔽

如何进行 DNS 屏蔽：

点击行为管理->DNS 定义->DNS 屏蔽，点击右上角的“新建”图标，输入 DNS 屏蔽组名，例如 ppstream，点击“确定”按钮。通过以上步骤，您已经新建了一个名为“ppstream”的 DNS 屏蔽组，如下图：



ID	组名	域名数目	引用数	状态	编辑
1	ppstream	0	0	<input checked="" type="checkbox"/>	

图 7-78：DNS 屏蔽列表界面

接下来，您可以点击编辑栏中的“修改”图标，对 ppstream 组中的 DNS 进行定义。



图 7-79：编辑域名屏蔽组界面

请点击右上角的“新建”图标，并在输入框中输入您希望屏蔽的 DNS。如下图：



图 7-80：新建域名屏蔽成员界面

例如我们输入“www.abcd.com”，依照此方式，您可以逐个加入您想要屏蔽的 DNS。

### ● DNS 免屏蔽

如何进行 DNS 免屏蔽：

DNS 免屏蔽功能是相当于 DNS 屏蔽功能而言的。例如您在 DNS 屏蔽中设置了屏蔽 “\*.abcd.com”，但你又不想屏蔽 “news.abcd.com”，那么该如何设置呢？

首先我们按照 DNS 屏蔽的设置步骤将 “\*.abcd.com” 加入到 DNS 屏蔽组中，接着我们依旧按照和 DNS 屏蔽类似的步骤来处理 “new.abcd.com” 这个免屏蔽域名，具体步骤如下：

点击行为管理->DNS 定义->DNS 免屏蔽，点击右上角的“新建”图标，输入 DNS 免屏蔽组名，例如 DNSEXEMPT1，点击“确定”按钮。通过以上步骤，您已经新建了一个名为 “DNSEXEMPT1” 的 DNS 免屏蔽组，如下图：



ID	组名	域名数目	引用数	状态	编辑
1	DNSEXEMPT1	0	0	<input checked="" type="checkbox"/>	

图 7-81：DNS 免屏蔽列表界面

接下来，您可以点击编辑栏中的“修改”图标，对 DNSEXEMPT1 组中的 DNS 进行定义。



编辑域名屏蔽组

组名

ID	域名/表达式	匹配类型	匹配数	状态	编辑
----	--------	------	-----	----	----

图 7-82：编辑域名屏蔽组界面

请点击右上角的“新建”图标，并在输入框中输入您希望免屏蔽的 DNS。如下图：



图 7-83: 新建域名免屏蔽成员界面

例如我们输入“news.abcd.com”，依照此方式，您可以逐个加入您想要免屏蔽的 DNS。

#### ◇ 网页定义

网页定义包括 URL 屏蔽和 URL 免屏蔽。

##### ● URL 屏蔽

如何进行 URL 屏蔽:

点击行为管理->URL 定义->URL 屏蔽，点击右上角的“新建”图标，输入 URL 屏蔽组名，例如 URLBLOCK1，点击“确定”按钮。通过以上步骤，您已经新建了一个名为“URLBLOCK1”的 URL 屏蔽组，如下图：

URL屏蔽		URL免屏蔽			
ID	组名	URL数目	引用数	状态	编辑
1	URLBLOCK1	0	0	<input checked="" type="checkbox"/>	
2	tieba	8	1	<input checked="" type="checkbox"/>	

图 7-84: URL 屏蔽列表界面

接下来，您可以点击编辑栏中的“修改”图标，对 URLBLOCK1 组中的 URL 进行定义。



图 7-85：编辑 URL 屏蔽组界面

请点击右上角的“新建”图标，并在输入框中输入您希望屏蔽的 URL。如下图：



图 7-86：编辑 URL 屏蔽成员界面

例如我们输入“http://lady.163.com/\*”，依照此方式，您可以逐个加入您想要屏蔽的 URL。

## ● URL 免屏蔽

URL 免屏蔽功能是相当于 URL 屏蔽功能而言的。例如您在 URL 屏蔽中设置了屏蔽“http://lady.163.com/\*”，但你又不想屏蔽“http://lady.163.com/special/\*”，那么该如何设置呢？

首先我们按照 URL 屏蔽的设置步骤将“http://lady.163.com/\*”加入到 URL 屏蔽组中，接着我们依旧按照和 URL 屏蔽类似的步骤来处理

“http://lady.163.com/special/\*” 这个免屏蔽 URL，具体步骤如下：

点击行为管理->URL 定义->URL 免屏蔽，点击右上角的“新建”图标，输入 URL 免屏蔽组名，例如 URLEXEMPT1，点击“确定”按钮。通过以上步骤，您已经新建了一个名为“URLEXEMPT1”的 URL 免屏蔽组，如下图：



ID	组名	URL数目	引用数	状态	编辑
1	URLEXEMPT1	0	0	<input checked="" type="checkbox"/>	

图 7-87：URL 免屏蔽列表界面

接下来，您可以点击编辑栏中的“修改”图标，对 URLEXEMPT1 组中的 URL 进行定义。



编辑 URL 免屏蔽组

组名

ID	URL	方式	匹配数	状态	编辑
----	-----	----	-----	----	----

图 7-88：编辑 URL 免屏蔽组界面

请点击右上角的“新建”图标，并在输入框中输入您希望免屏蔽的 URL。如下图：



新建 URL 免屏蔽成员

URL

方式

状态

图 7-89：新建 URL 免屏蔽成员界面

例如我们输入“http://lady.163.com/special/\*”，依照此方式，您可以逐个加入您想要免屏蔽的 URL。

## ◇ 文件定义

文件定义包括文件类型屏蔽，其依据文件的后缀名对文件进行过滤。目前支持的能够对文件后缀名进行过滤的协议有四种：HTTP、FTP、SMTP 和 POP3。

### ● 文件类型屏蔽

如何进行文件类型屏蔽

点击行为管理->文件定义->文件类型屏蔽，点击右上角的“新建”图标，输入文件类型屏蔽组名，例如 FILEBLOCK1，点击“确定”按钮。通过以上步骤，您已经新建了一个名为“FILEBLOCK1”的文件屏蔽组，如下图：



文件类型屏蔽					
ID	组名	文件数	引用数	状态	编辑
1	FILEBLOCK1	0	0	<input checked="" type="checkbox"/>	

图 7-90：文件类型屏蔽列表界面

接下来，您可以点击编辑栏中的“修改”图标，对 FILEBLOCK1 组中的文件类型进行定义。



文件类型屏蔽					
编辑文件类型屏蔽组					
组名	<input type="text" value="FILEBLOCK1"/>	<input checked="" type="checkbox"/>	<input type="button" value="确定"/>		
ID	文件类型	HTTP	FTP	SMTP	POP3

图 7-91：编辑文件类型屏蔽组界面

请点击右上角的“新建”图标，并在输入框中输入您希望屏蔽的文件类型。如下图：



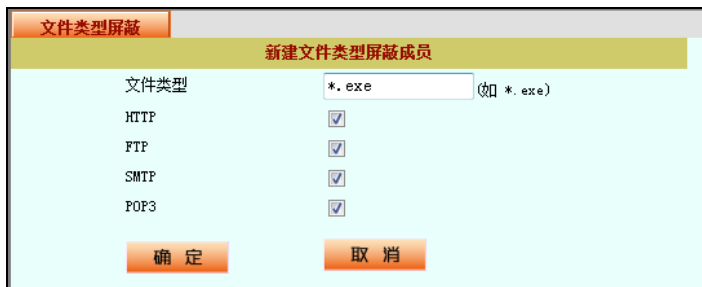


图 7-92: 新建文件类型屏蔽成员界面

例如我们输入“\*.exe”，然后选择相关协议，依照此方式，您可以逐个加入您想要屏蔽的文件类型。

#### ◇ 邮件审计

Anysec 设备具备邮件延迟审计功能，当内网用户使用邮件客户端通过 SMTP 协议发送邮件时，如果防火墙策略匹配到该用户所发送的邮件需要进行延迟审计后才能发送，那么该用户所发送的邮件将被 Anysec 临时收藏起来，待邮件审核员对该邮件进行审计通过后，该邮件才能发送出去。而这一切对于刚才发送邮件的用户来说是完全透明的。当有邮件需要审计时，Anysec 系统会依据审计配置向审计员发送一封提示邮件，以告知审计员及时处理邮件以免耽误他人工作。

Anysec 邮件审计功能包含三个部分：

#### ● 发件审计

用户发送的所有需要审计的邮件都会存放在发件审计列表中，一般情况下，只有当审计通过后，该邮件才会发往 Internet。

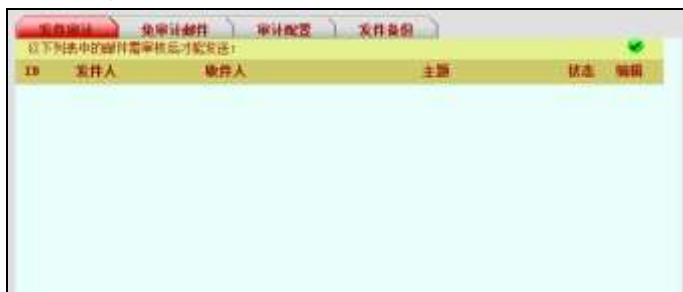


图 7-93: 发件审计列表界面

- **免审计邮件**

免审计邮件用于对一些特殊的邮件发送人或接收人进行免审计处理，发件人或接收人必须至少输入一项。



图 7-94：新建发件白名单界面

- **审计配置**



图 7-95：新建发件审计配置界面

- **SMTP 服务器：**指发送审计提示邮件使用的 SMTP 服务器地址。
- **源邮件地址：**指发送审计提示邮件的源地址。
- **审计员邮箱：**审计员接收提示审计邮件的 Email 地址

当 SMTP 服务器需要验证用户名和密码时，您可以勾选复选框，并输入登录用户名和密码。

➤ **邮件审计策略：**

当需要审计的邮件由于某种原因未能及时审计发送时，该审计邮件将会依照邮件审计策略进行处理：自动发送或删除。

● **发件备份（高端设备具有）**



图 7-96：新建发件备份列表界面

将邮件备份在 ANYSEC 安全网关中。

## ◇ 带宽控制

Anysec 产品提供一种非常简易的带宽控制功能以处理由于 P2P 等软件造成带宽滥用而影响正常的网络工作，您只需要简单的指定 IP 地址，并设置其最大带宽即可。**注意：该功能主要用于处理非正常情况造成的网络带宽滥用，该功能设置的 IP 带宽在设备重启后将不再有效。**如果您需要对网络带宽进行有效管理，您可以通过防火墙的策略来对带宽进行定义。

下图为新建 IP 带宽管理界面。



图 7-97：新建 IP 带宽管理设置界面

## ○ 网络监控

网络监控功能是 Anysec 设备的特色功能之一，您可以通过该功能了解内网用户的上网情况。

支持哪些网络监控？

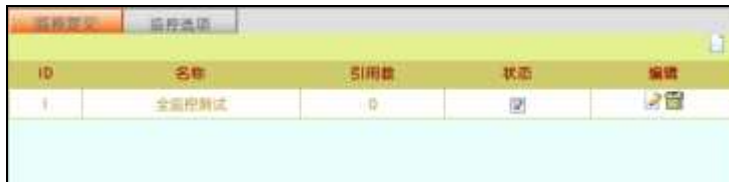
Anysec 设备支持以下网络监控功能：

### ◇ 定义监控规则

点击网络监控->监控规则菜单，可以配置网络监控策略。

**注意：您的网络监控策略需要在防火墙的访问控制中引用才能生效。**

- 查看监控规则



ID	名称	引用数	状态	编辑
1	全网检测	0	<input type="checkbox"/>	

图 7-118：流量规则列表

**ID：**监控规则序号。

**名称：**监控规则名称，被防火墙策略采用。

**引用数：**监控规则被防火墙策略引用的次数。

**状态：**监控规则当前是否被激活的状态。

- 新建监控规则

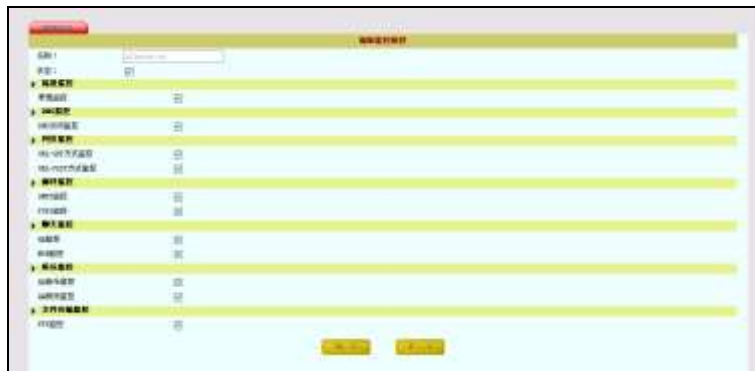


图 7-119：新建监控规则界面

- ◇ 监控选项

Anysec 设备支持远程存储监控日志



图 7-125: 监控选项界面

若选择远程存储日志服务器，请先确认远程存储服务器进程是否已启动。

#### ◇ 流量监控（具体功能依产品型号不同而不同）

Anysec 能对每个 IP 的网络流量进行记录和统计，并以图表的形式直观的展示出来。Anysec 设备能显示实时带宽、5 分钟流量统计、小时流量统计、日流量统计和月流量统计。

##### ● 实时带宽：

实时带宽	5分钟流量								小时流量		日流量		月流量	
	IP/用户	总速率	发送速率	接收速率	TCP速率	UDP速率	ICMP速率	HTTP速率	其它					
	192.168.118.100	21.0KB/S	21.0KB/S	1.1KB/S	200B/S	22.0KB/S	0B/S	0B/S	0B/S					
	总计	22.0KB/S	21.0KB/S	1.1KB/S	200B/S	22.0KB/S	0B/S	0B/S	0B/S					

图 7-100: 实时带宽列表

##### ● 5 分钟流量统计表：

实时带宽	5分钟流量								小时流量		日流量		月流量	
	IP/用户	总量	发送总量	接收总量	TCP协议	UDP协议	ICMP协议	HTTP协议	其它					
	192.168.118.100	9.2M	2.3M	7.0M	7.2M	2.1M	0	7.2M	0					
	总计	9.2M	2.3M	7.0M	7.2M	2.1M	0	7.2M	0					

图 7-101: 5 分钟流量统计表

● 小时流量统计图：

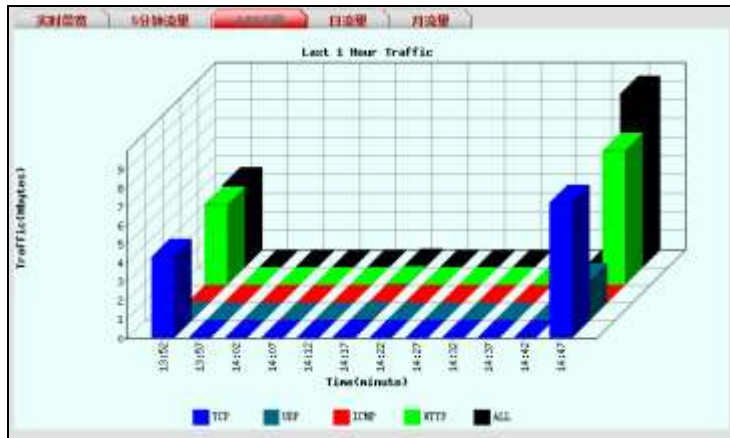


图 7-102：小时流量统计图

● 日流量统计图：

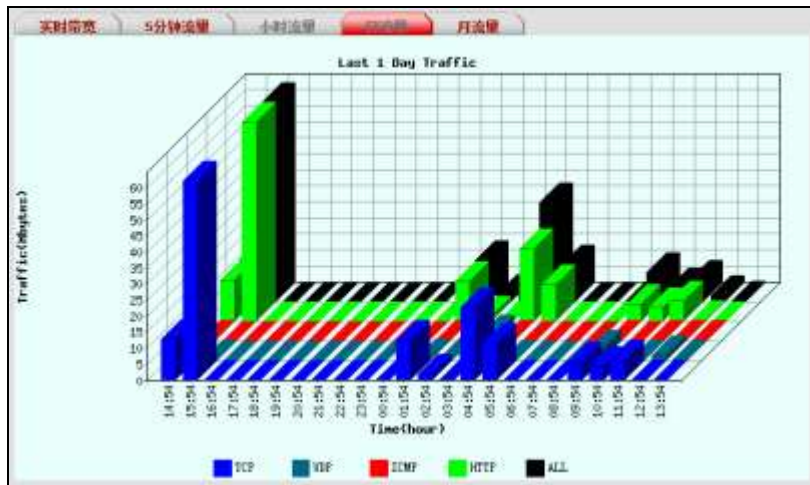


图 7-103：日流量统计图

● 月流量统计图：



图 7-104：月流量统计图

◇ DNS 监控

Anysec 设备能监控并记录内网用户所有 DNS 请求情况：（型号不同表现形式会有不同），中端型号一般只显示最新的 200 条 DNS 访问信息，一般高端型号能够依据日期进行 DNS 访问记录，并能内网 IP 来查询其所以访问过的 DNS，同时也可以通过 DNS 来查询哪些内网 IP 用户访问过该 DNS。

ID	内网用户	时间	域名
1	100.100.98.127	Fri Jan 22 10:43:50 2010	10.100.98.127
2	100.100.98.127	Fri Jan 22 10:43:51 2010	10.100.98.127
3	100.100.98.127	Fri Jan 22 10:43:51 2010	adk.sina.com.cn
4	100.100.98.127	Fri Jan 22 10:43:51 2010	adk.sina.com.cn
5	100.100.98.127	Fri Jan 22 10:43:51 2010	kg.sina.com.cn
6	100.100.98.127	Fri Jan 22 10:43:51 2010	www.sina.com.cn
7	100.100.98.127	Fri Jan 22 10:43:51 2010	www.sina.com.cn
8	100.100.98.127	Fri Jan 22 10:43:51 2010	kg.sina.com.cn
9	100.100.98.127	Fri Jan 22 10:43:50 2010	www.sina.com.cn
10	100.100.98.127	Fri Jan 22 10:43:50 2010	www.sina.com.cn
11	100.100.98.127	Fri Jan 22 10:43:50 2010	10.100.98.127
12	100.100.98.127	Fri Jan 22 10:43:50 2010	10.100.98.127
13	100.100.98.127	Fri Jan 22 10:43:50 2010	10.100.98.127
14	100.100.98.127	Fri Jan 22 10:43:50 2010	10.100.98.127

图 7-105：DNS 监控列表





## ◇ 邮件监控

Anysec 设备能监控并记录内网用户所有邮件发送和邮件接收情况：（型号不同表现形式会有不同），中端型号一般只显示最新的 200 条邮件信息，一般高端型号能够依据日期进行邮件记录，并能内网 IP 来查询其所有发送和接收过的邮件。

### ● 已发邮件（SMTP）：



编号	IP 地址	日期	发件人	收件人	主题
1	192.168.1.100	Thu Dec 1 00:00:00 2010	msn@china.net	100@163.com	test

图 7-108：已发邮件列表

### ● 已收邮件（POP3）：



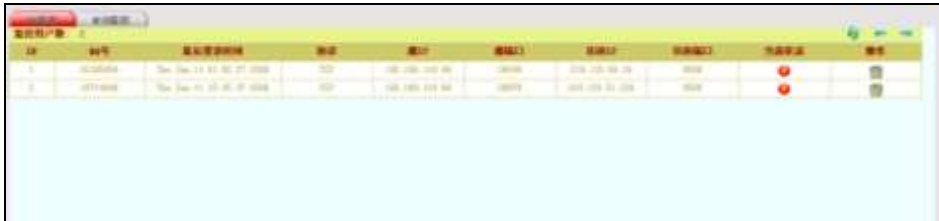
编号	IP 地址	日期	发件人	收件人	主题
1	192.168.1.100	Thu Dec 01 00:00:00 2010	100@163.com	100@163.com	test mail

图 7-109：已收邮件列表

## ◇ 聊天监控

Anysec 设备能监控并记录 QQ 和 MSN 等即时聊天软件的使用情况，对于 QQ 软件，Anysec 能实时获取该 IP 用户所使用的聊天 QQ 号以及查看当前 QQ 是否在线。对应 MSN 软件，Anysec 设备不仅能获取该 IP 用户的 MSN ID 号，并且能记录 MSN 双方的聊天记录。


- **QQ 监控:**



IP	用户名	最后登录时间	状态	源IP	源端口	目标IP	目标端口	连接状态	操作
1	10200004	Thu Nov 11 02:32:27 2009	活跃	192.168.1.100:80	20000	192.168.1.100:80	8000	●	删除
2	10200004	Thu Nov 11 02:32:27 2009	活跃	192.168.1.100:80	20000	192.168.1.100:80	8000	●	删除

图 7-110: QQ 监控列表

- **MSN 监控**



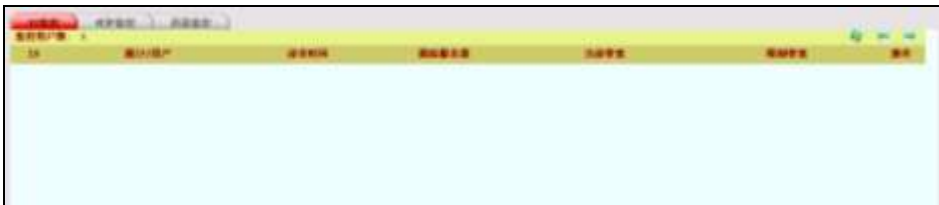
IP	用户名	最后登录时间	状态	源IP	源端口	目标IP	目标端口	连接状态	操作
1	10200004	Thu Nov 11 02:32:27 2009	活跃	192.168.1.100:80	20000	192.168.1.100:80	8000	●	删除

图 7-111: MSN 监控列表

- ◇ **P2P 监控**

Anysec 设备能够对目前流行的 P2P 下载工具 BT、电驴以及迅雷实时报告, 管理员可以通过该功能及时获取内网 IP 用户对 P2P 软件的使用情况。

- **BT 监控**



IP	用户名	最后登录时间	状态	源IP	源端口	目标IP	目标端口	连接状态	操作
----	-----	--------	----	-----	-----	------	------	------	----

图 7-112: BT 监控列表

- 电驴监控

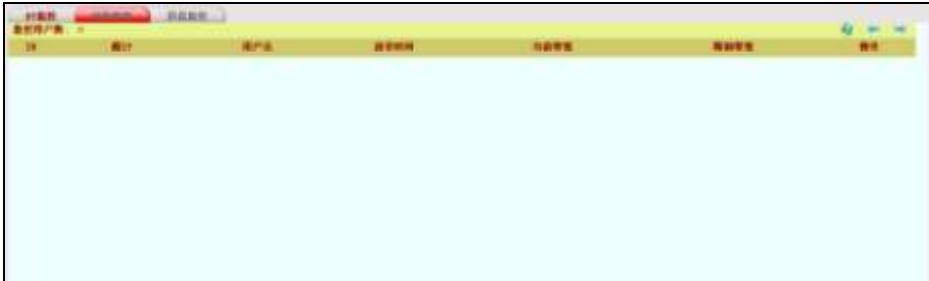


图 7-113: 电驴监控列表

- 迅雷监控

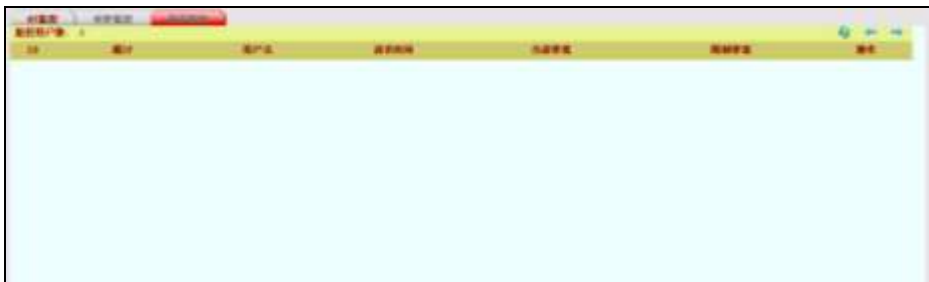


图 7-114: 迅雷监控列表

- ◇ 娱乐监控

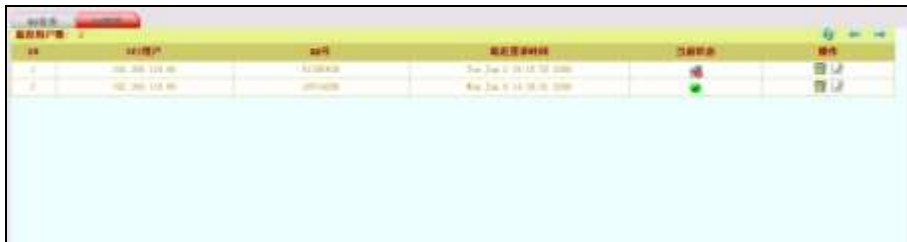
Anysec 设备能对 QQ 音乐及 QQ 游戏进行实时监控。管理员能通过该功能获取当前 IP 用户的 QQ 音乐和 QQ 游戏的使用情况。

- QQ 音乐



图 7-115: QQ 音乐监控列表

- QQ 游戏

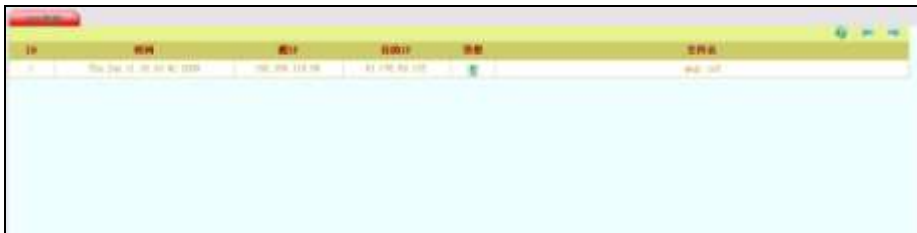


序号	IP地址	用户名	最近登录时间	当前状态	操作
1	192.168.1.100	12345678	Thu, Jun 11 08:12:12 2009	●	删除
2	192.168.1.100	87654321	Thu, Jun 11 14:30:12 2009	●	删除

图 7-116: QQ 游戏监控列表

- ◇ FTP 监控

Anysec 设备能够监控内网 IP 用户使用 FTP 协议进行文件上传下载情况。



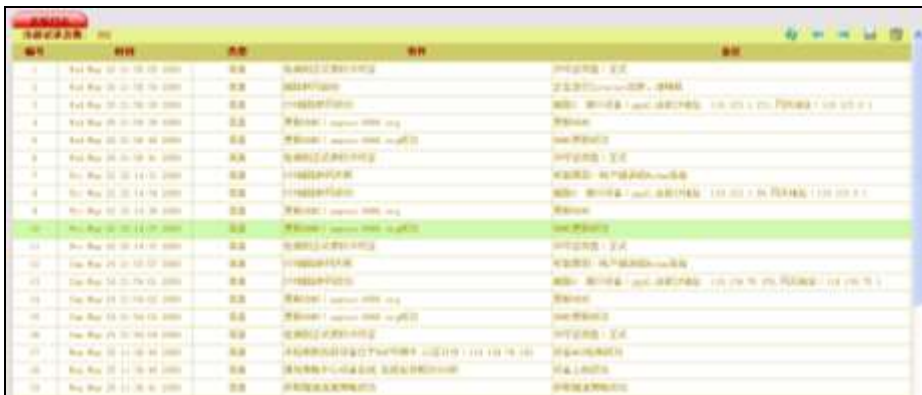
IP	时间	源IP	目标IP	类型	文件大小
1	Thu, Jun 11 08:12:12 2009	192.168.1.100	81.192.84.112	●	940.107

图 7-117: FTP 监控列表

- 日志审计

Anysec 设备提供了多种日志，您可以通过查看日志信息获取系统的各种日志：

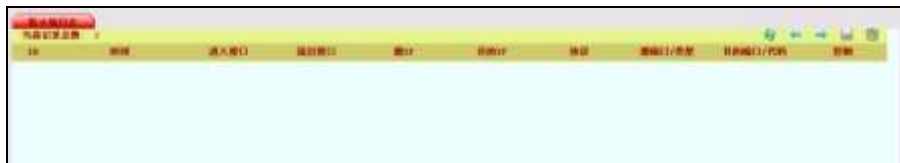
### ◇ 系统日志



编号	时间	类型	事件	备注
1	Wed May 26 22:18:18 2009	成功	策略组日志策略执行成功	策略组策略组：无策略
2	Wed May 26 22:18:18 2009	成功	策略组执行成功	策略组策略组：无策略
3	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
4	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
5	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
6	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
7	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
8	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
9	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
10	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
11	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
12	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
13	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
14	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
15	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
16	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
17	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
18	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
19	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
20	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
21	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
22	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
23	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
24	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
25	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
26	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
27	Wed May 26 22:18:18 2009	成功	策略组策略组执行成功	策略组策略组：无策略
28	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略
29	Wed May 26 22:18:18 2009	成功	策略组策略组：system-2009-log	策略组策略组：无策略

图 7-120：系统日志列表

### ◇ 防火墙日志



时间	源IP	目的IP	源端口	目的端口	协议	源地址/子网	目的地址/子网	策略
[Empty table content]								

图 7-121：防火墙日志列表

### ◇ VPN 日志


#### ● 点点通日志



编号	时间	源IP	目的IP	源端口	目的端口	策略
[Empty table content]						

图 7-122：点点通日志列表

- PPTP 日志



The screenshot shows a web-based interface for viewing PPTP logs. At the top, there are several tabs: '系统日志', 'pptp日志', 'ipsec日志', 'ssl日志', and '移动客户端日志'. The 'pptp日志' tab is currently selected and highlighted in red. Below the tabs is a table with a yellow header and a light blue body. The header row contains the following columns: '编号' (ID), '时间' (Time), '操作' (Action), and '备注' (Remarks). The table body is currently empty.

图 7-124: PPTP 日志列表

- IPSEC 日志



The screenshot shows a web-based interface for viewing IPSEC logs. At the top, there are several tabs: '系统日志', 'pptp日志', 'ipsec日志', 'ssl日志', and '移动客户端日志'. The 'ipsec日志' tab is currently selected and highlighted in red. Below the tabs is a table with a yellow header and a light blue body. The header row contains the following columns: '编号' (ID), '时间' (Time), '操作' (Action), and '备注' (Remarks). The table body is currently empty.

图 7-123: IPSEC 日志列表

- SSL 日志



The screenshot shows a web-based interface for viewing SSL logs. At the top, there are several tabs: '系统日志', 'pptp日志', 'ipsec日志', 'ssl日志', and '移动客户端日志'. The 'ssl日志' tab is currently selected and highlighted in red. Below the tabs is a table with a yellow header and a light blue body. The header row contains the following columns: '编号' (ID), '时间' (Time), '操作' (Action), and '备注' (Remarks). The table body is currently empty.

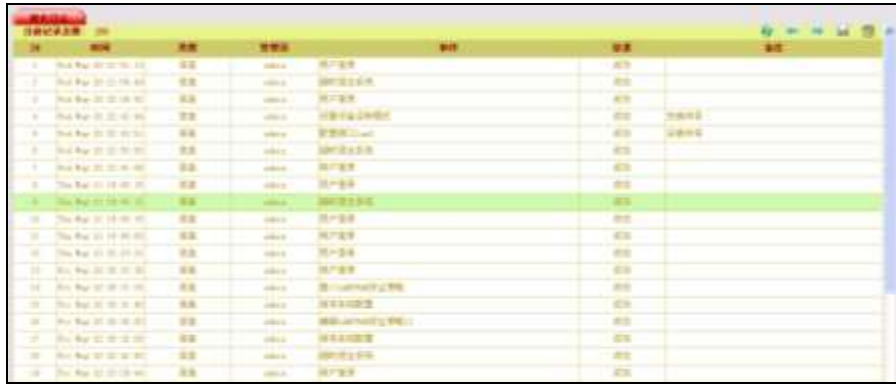
- 移动客户端日志



The screenshot shows a web-based interface for viewing mobile client logs. At the top, there are several tabs: '系统日志', 'pptp日志', 'ipsec日志', 'ssl日志', and '移动客户端日志'. The '移动客户端日志' tab is currently selected and highlighted in red. Below the tabs is a table with a yellow header and a light blue body. The header row contains the following columns: '编号' (ID), '时间' (Time), '操作' (Action), and '备注' (Remarks). The table body is currently empty.

图 7-124: 移动客户端日志列表

- 操作日志



ID	时间	类型	用户名	事件	结果	备注
1	Thu Aug 21 22:28:23	登录	admin	用户登录	成功	
2	Thu Aug 21 22:28:24	登录	admin	清除日志记录	成功	
3	Thu Aug 21 22:28:25	登录	admin	用户登录	成功	
4	Thu Aug 21 22:28:26	登录	admin	设置设备名称和地址	成功	设备名称
5	Thu Aug 21 22:28:27	登录	admin	设置设备名称	成功	设备名称
6	Thu Aug 21 22:28:28	登录	admin	清除日志记录	成功	
7	Thu Aug 21 22:28:29	登录	admin	用户登录	成功	
8	Thu Aug 21 22:28:30	登录	admin	清除日志记录	成功	
9	Thu Aug 21 22:28:31	登录	admin	清除日志记录	成功	
10	Thu Aug 21 22:28:32	登录	admin	清除日志记录	成功	
11	Thu Aug 21 22:28:33	登录	admin	清除日志记录	成功	
12	Thu Aug 21 22:28:34	登录	admin	清除日志记录	成功	
13	Thu Aug 21 22:28:35	登录	admin	清除日志记录	成功	
14	Thu Aug 21 22:28:36	登录	admin	清除日志记录	成功	
15	Thu Aug 21 22:28:37	登录	admin	清除日志记录	成功	
16	Thu Aug 21 22:28:38	登录	admin	清除日志记录	成功	
17	Thu Aug 21 22:28:39	登录	admin	清除日志记录	成功	
18	Thu Aug 21 22:28:40	登录	admin	清除日志记录	成功	
19	Thu Aug 21 22:28:41	登录	admin	清除日志记录	成功	
20	Thu Aug 21 22:28:42	登录	admin	清除日志记录	成功	

图 7-127: 操作日志列表

- ◇ 日志配置

Anysec 设备支持本机日志和远程 syslog 日志



图 7-125: 日志设计界面

若选择远程日志，请先确认远程 SYSLOG 服务器进程是否已启动。



## 第八章 Console 配置

ANYSEC 系列产品支持 Console 配置方式，本章介绍如何使用 Windows 系统超级终端控制台程序配置设备。

### ➔ 连接

Console 配置方式硬件接线图示：



图 8-1：Console 配置连接图

### ➔ 配置电脑

以 Windows XP 为例。在“开始”“程序”“附件”“通讯”“超级终端”，启动超级终端。

- 1、新建连接，新建 anysec，如下图示：



图 8-2: 新建连接名称设置-1

2、 选择正确的 COM 口，根据实际连接接口，选择正确的 COM 口（连接计算机使用的串口），如下图示：



图 8-3: 新建连接名称设置-2

3、 COM 口属性配置。如下图示：



图 8-4: 调整 COM 口属性界面

## ② 基本配置

系统正常引导启动后。初次登陆配置，在提示登陆处输入缺省账号：

ANYSEC Login:admin

Password:anysec （密码输入为隐藏状态，无显示）

成功登陆后，显示如下：

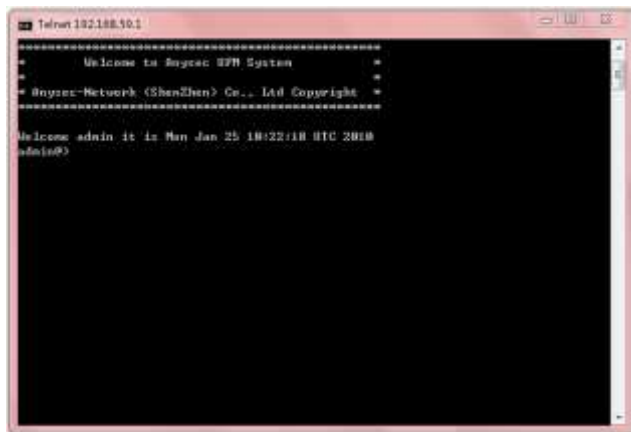


图 8-5: Telnet 登陆界面

输入 # 回车, 显示主菜单, 显示如下:



图 8-6: Telnet 下配置界面

## 第九章 常见问题解答

本章列举了部分常见的问题。更多 FAQ，敬请参考 [www.anysec.com](http://www.anysec.com)。

### ➤ 忘记密码怎么办？

ANYSEC 系列产品在后面板有 Reset 键，按住几秒钟后，前面板 system 第四盏灯亮起，则登陆地址、用户名、密码会恢复为默认。也可以通过串口登陆设备并重启设备，在重启过程中按“i”键，用户名、密码同样会恢复为默认。

### ➤ 如何查看当前设备接口状态及其 IP 地址？

在 WEB 管理界面，进入“系统管理”——“网络管理”——“接口”可以看到各个接口的 IP 地址及连接状态等信息了。

### ➤ 如何确认自动隧道已成功建立？

使用点点通时，点击“VPN 管理”——“点点通”——“隧道监控”——“测试”。如果隧道建立成功测试结果正常。

### ➤ 局域网不能上网如何处理？

1. 请先查看电脑到网关之间是否通畅。
2. 如果通畅查看面板的 WAN 和 system 指示灯状态：如果 WAN 等不亮或 system 灯为左灯灭，右灯闪烁，此时为外网故障。请检查 Anysec 外网线连接是否正常；重启 Anysec 设备或 Modem。如果还不能恢复正常，请使用单台电脑上网是否正常，如果不正常，请联系运营商解决。

### ➤ 能上网但不能和其他节点的主机或服务器通信，该如何处理？

A 点击 Web 管理界面的“VPN 管理”-“点点通”-“隧道监控”查看隧道是否正常。

### ➤ ADSL 无法拨号上网

- 1、检查线路是否松动
- 2、检查 ADSL 账户和密码是否填写正确
- 3、部分地区的 ADSL 用户，在终端设备突然断电后，不能马上拨号。需要等待一段时间才能重新连接。
- 4、确认 Modem 是处于路由模式还是透明模式。Modem 如是路由模式请修改为透明模式，由 Anysec 设备进行 PPPoE 拨号。

### ➤ ADSL 线路很不稳定，常常断线怎么办？

当前 ADSL 一般使用 PPPoE 拨号，拨号成功后拨号程序会不断地发送 LCP（链路控制协议）包来维护 PPP 连接。如果 ADSL 线路过长，或者线路质量不好，ADSL Modem 故障等，都容易导致 LCP 数据包发送和接收异常，造成连接中断。

- 1、检查内网是否有病毒造成大量往外发包，或者内网有使用 BT 等 P2P 工具下载造成上下行数据量较大，或者内部计算机较多正常访问量很大，ADSL 不能满足带宽要求等。这些情况都容易导致 ADSL 出现断线重拨。
- 2、ADSL 线路本身不稳定，容易断线重拨。可以使用电脑拨号进行验证。线路问题请及时联系线路服务商获得支持。

## ➤ 故障处理流程

当内网 PC 无法连接 Internet 时，首先检查设备是否已正常连接 Internet，处理流程参考如下：

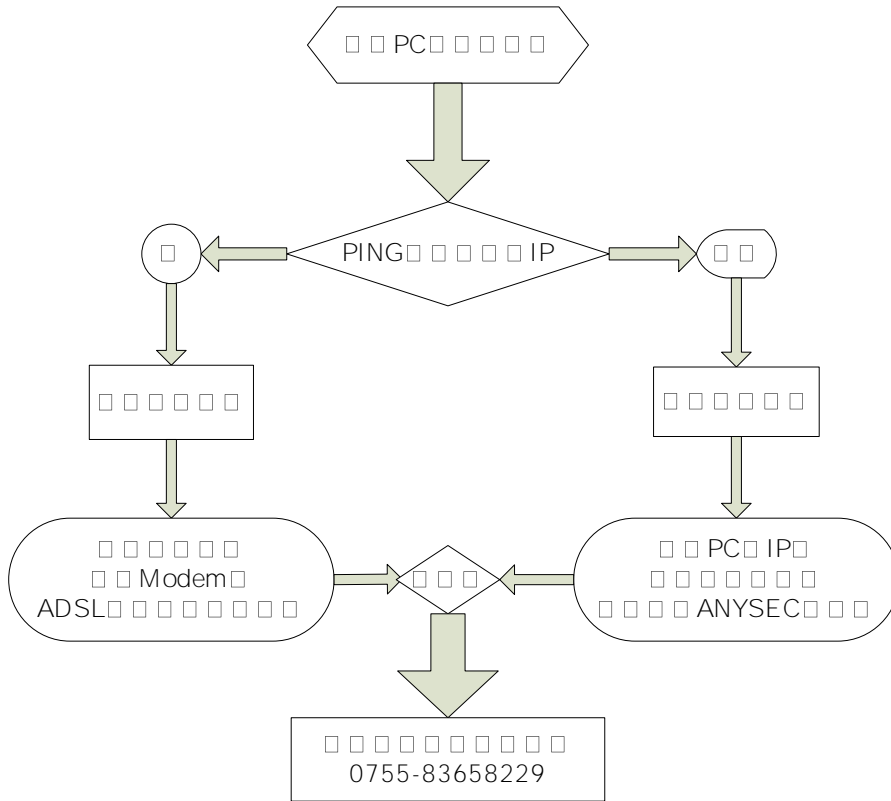


图 9-1：设备故障处理流程图

## 附：点点通配置实例

本章将以实例讲解点点通配置过程，本实例是在 ANYSEC 设备通过智能安装向导配置后，设备已经正常运行，进行单独配置点点通 VPN 互联模块为目的。分为中心点和分支节点两部分介绍。

### ☞ 客户背景介绍

- **总部中心点：**

ANYSEC 设备作为网关，通过固定 IP 上网；

内网网段：192.168.1.0，网关地址：192.168.1.1，掩码：255.255.255.0。

- **分支节点 A：**

ANYSEC 设备作为网关，通过 ADSL 上网；

内网网段：192.168.2.0，网关地址：192.168.2.1，掩码：255.255.255.0。

### ☞ 总部点点通管理平台配置

1、点击“VPN 管理”——“点点通”——“设备管理”，如下图所示



序号	设备名	设备ID	内网口IP	隧道子网	联网方式	在线生存期 (秒)	备注	编辑
----	-----	------	-------	------	------	-----------	----	----

图附-1



- 2、点击右上角“新建”添加设备，现将总部中心点设备添加至点点通平台。如下图所示：

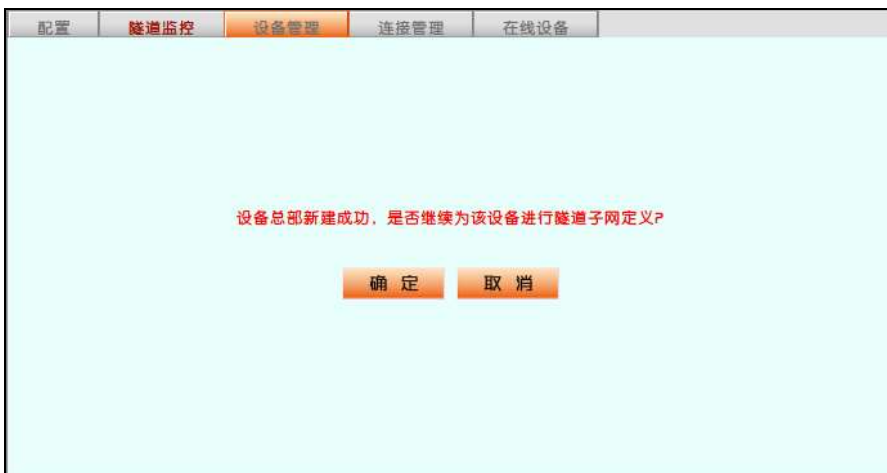


配置	隧道监控	设备管理	连接管理	在线设备
<b>新建设备</b>				
设备名	总部			
设备ID	1000			
通讯密码	●●●●●●			
联网模式	静态公网IP			
IP地址	123.123.123.123			
内网口IP	192.168.1.1			
在线生存期	300 (120-3600秒)			
联系人	工程师			
电话	13510693536			
备注	总部设备			
<input type="button" value="确定"/> <input type="button" value="取消"/>				

图附-2

注意：联网模式请根据实际情况填写，拥有固定 IP 上网方式，请选择静态公网 IP；ADSL 上网方式或接在内网交换机下时，请选择“动态公网 IP 或 NAT 后”。此处根据客户实际情况，我们选择“静态公网 IP”，并将公网 IP 地址填入“IP 地址”栏（动态公网 IP 没有此项）。**内网口 IP**：指该设备所在网络内网网口 IP 地址。

- 3、点击“确定”，系统会提示是否继续为该设备进行隧道，点击“确定”。如下图所示：



配置	隧道监控	设备管理	连接管理	在线设备
设备总部新建成功，是否继续为该设备进行隧道子网定义?				
<input type="button" value="确定"/> <input type="button" value="取消"/>				

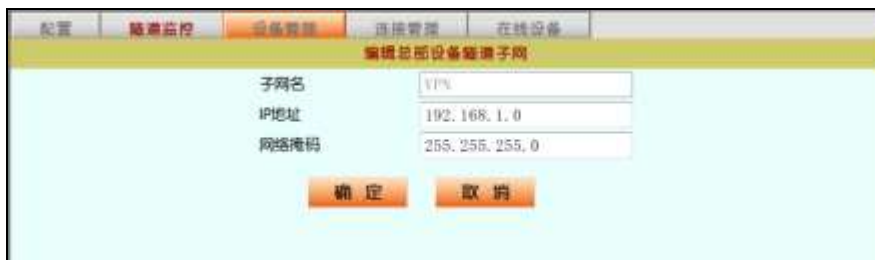
图附-3

- 4、点击“确定”后，进入隧道子网列表，点击右上角“新建”图标，添加隧道子网，如下图所示：



图附-4

- 5、点击“新建”后，填写子网名（任意填写），IP 地址：该设备内网网段，如 192.168.1.0，子网掩码填写：255.255.255.0。如下图所示：



图附-5

- 6、点击“确定”，进入设备管理列表，列表中显示已添加过的设备。如下图所示：



图附-6

- 7、点击右上角“新建”再继续添加设备，现将分支节点设备添加至点点通平台。如下图所示：



配置	隧道监控	设备管理	连接管理	在线设备
新建设备				
设备名	北京分部			
设备ID	1001			
通讯密码	●●●●●●			
联网模式	动态公网IP或NAT设备后			
内网IP	192.168.2.1			
在线生存期	300 (120-3600秒)			
联系人	北京网管			
电话	13713867534			
备注	北京分公司网管			
<input type="button" value="确定"/> <input type="button" value="取消"/>				

图附-7

- 8、点击“确定”，系统再次提示是否进入隧道子网配置，点击“确定”，新建该设备的隧道子网，填写子网名（任意填写），IP地址：该设备内网网段，如192.168.2.0，子网掩码填写：255.255.255.0。如下图所示：



配置	隧道监控	设备管理	连接管理	在线设备
新建北京分部设备隧道子网				
子网名	VPS			
IP地址	192.168.2.0			
网络掩码	255.255.255.0			
<input type="button" value="确定"/> <input type="button" value="取消"/>				

图附-8

- 9、点击“确定”，进入设备管理列表，列表中显示已添加过的设备。如下图所示：

配置									
设备管理									
连接管理									
在线设备									
序号	设备名	设备ID	内网IP	连接子网	联网方式	在线生存期(秒)	备注	编辑	
1	总部	1000	192.168.1.1	192.168.1.0/255.255.255.0	静态公网IP	300	总部设备		
2	北京分部	1001	192.168.2.1	192.168.2.0/255.255.255.0	动态公网IP/PPPT 设备ID	300	北京分公司 网关		

图附-9

- 10、 点击“连接管理”，进入设备列表后，点击“总部”设备后面编辑选项中的“修改连接策略”，如下图所示：

配置									
设备管理									
连接管理									
在线设备									
ID	设备名	连接数		编辑					
1	总部	0							
2	北京分部	0							

图附-10

- 11、 点击“修改连接策略”后，进入编辑界面，将左侧列表中的“北京分部”选上，点击中间的“向右添加”按钮，将“北京分部”添加至“总部”设备的连接设备列表中。如下图所示：



图附-11

- 12、 点击“确定”后，返回连接设备列表界面，在此处可以看到每台设备的连接隧道数。如下图所示：

ID	设备名	隧道数	编辑
1	总部	1	
2	北京分部	1	

图附-12

- 13、 设备添加完成后，下一步将激活点点通策略中心，点击“配置”，填入总部中心点的设备名、设备 ID、通讯密码、隧道策略寻址方式、策略中心地址，并勾选“现在激活”选项。如下图所示：



图附-13

点击“确定”，系统会提示“上线成功”。至此，点点通中心点设备配置完成。通过点点通“隧道监控”，可以测试隧道是否建立成功；通过“在线设备”，可以查看所有设备是否在线、所有设备公网 IP、进行远程管理、下发策略等。如下两图所示：

ID	设备ID	设备名	连接方式	名称	隧道网段	当前状态	隧道性	操作
1	1000	device1	高速连接		192.168.118.0/255.255.255.0	🟢	🟢	🔄
2	1001	device2	直接连接		192.168.0.0/255.255.255.0	🟡	测试	🔄
3	1004	device5	直接连接		192.168.88.0/255.255.255.0	🟡	测试	🔄
4	1005	device6	高速连接			🟡	测试	🔄

图附-14

ID	设备名	设备ID	认证IP	NAT后	更新时间	在线生存期 (秒)	当前状态	操作
1	device2	1002	219.133.88.40	否	Fri Jan 22 09:37:10 2010	300	🟢	🔍 🔄 🗑️
2	北京办事处	1005	114.117.14.45	否	Fri Jan 22 09:35:26 2010	300	🟢	🔍 🔄 🗑️

图附-15

### 🔍 分支节点配置：

点击“VPN 管理”——“点点通”——“配置”。如下图所示：



图附-16

填写由总部下发的设备名、设备 ID、通讯密码（即中心点点通管理平台添加在线设备时，填写的信息），此例中应填入设备名：北京分部，设备 ID：1001，设备密码：\*\*\*\*\*。

隧道策略寻址方式：当总部为固定 IP 或域名时，填写 IP 或域名，当总部使用 SecROS 网络平台寻址时，填写我司授权给中心点设备的 SecROS 简域即可。

勾选“现在激活”，点击确定。如果信息填写正确，系统会提示上线成功；如果信息填写错误，系统会提示**“隧道策略获取失败，请检查设备主机名、设备 ID、密码以及策略中心设置是否配置正确！”**。

设备成功上线后，可以在隧道监控中查看隧道连接状态，并可测试隧道连通性。

注意：当总部中心点没有固定 IP 时，推荐使用我司拥有自主知识产权的 SecROS 认证平台进行寻址互联，更加稳定、安全、快速。若采用点点通平台，仅需在隧道策略寻址方式项，选择“通过 SecROS 网络平台寻址”，在“策略中心地址”中，填入由我司授权给您的“简域名称”即可。